ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія захисту кінцевих точок на базі рішення Symantec Endpoint Protection»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Міщан В.Є.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

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.
“___”_____ 2020 року

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

Міщану Володимиру Євгеновичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія захисту кінцевих точок на базі рашення Symantec Endpoint Protection»

керівник магістерської роботи Гайдур Галина Іванівна, д.т.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «10» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2020 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
розгорнуте рішення Symantec Endpoint Protection;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз сучасних завдань та вимог до продуктів Endpoint Protection Platform.
2. Дослідження конкуренції на ринку Endpoint Protection Platform та визначення тенденцій їх розвитку
3. Вивчення технологій та функціональних можливостей Symantec Endpoint Protection

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

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

3. Моделі розгортання та обслуговування хмар.

4. Переваги використання хмарних сервісів.

5. Проблеми кібербезпеки хмарних сервісів.

6. Зона відповідальності постачальника та користувача хмарних сервісів стандарту NIST SP 500-292.

7. Завдання щодо забезпечення безпеки використання хмар.

8-9. Принцип роботи CASB.

11. Архітектура Microsoft Cloud App Security.

10. Етапи розгортання Microsoft Cloud App Security.

11.Технологія виявлення і контролю тіньових IT у мережі.

12. Висновки за результатами роботи.

6. Дата видачі завдання 01.10.2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми атак на кінцеві точки	09.10.2020 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.10.2020 р.	
3.	Аналіз сучасних завдань та вимог до продуктів Endpoint Protection Platform	16.11.2020 р.	
4.	Дослідження конкуренції на ринку Endpoint Protection Platform та визначення тенденцій їх розвитку	23.11.2020 р.	
5.	Розроблення рекомендацій щодо застосування технології захисту кінцевих пристроїв на базі рішення Symantec Endpoint Protection	02.12.2020 р.	
6.	Оформлення результатів дослідження.	09.12.2020 р.	
7.	Підготовка доповіді до захисту.	15.12.2020 р.	

Студент Міщан В. Є.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 59 сторінок, 11 рисунків, 10 джерел.

Об'єкт дослідження – процес забезпечення захисту інформаційної системи за допомогою Symantec Endpoint Protection.

Предмет дослідження – технологія забезпечення захисту інформаційної системи за допомогою Symantec Endpoint Protection.

Мета роботи – дослідити можливості захисту корпоративних мереж за допомогою Symantec Endpoint Protection та розробити рекомендації щодо застосування технології на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації та рекомендацій розробника, експертних рішень та їх порівняння.

В роботі проведено аналіз ринку продуктів Endpiont Security, більш детально розглянуто на прикладі Symantec Endpoint Protection та визначено мета та завдання.

Досліджено технології забезпечення захисту інформаційних систем на прикладі рішення Symantec Endpoint Protection. Визначено призначення, основні функції та принципи роботи рішення Symantec Endpoint Protection.

На основі досліджень проведених в роботі визначено функціональні можливості рішень Endpoint Security, стан конкуренції на сучасному ринку, тенденції та вектори їх розвитку.

Галузь використання – захист кінцевих пристроїв.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, АНТИВІРУС, КІНЦЕВИЙ ПРИСТРІЙ, ТЕХНОЛОГІЯ ЗАХИСТУ, СКАНУВАННЯ, ВРАЗЛИВІСТЬ, ЗАГРОЗА, КОНТРОЛЬ ТРАФІКУ

ЗМІСТ

Стор.

ВСТУП

Кінцеві пристрої завжди були якщо не головним, то одним з основних джерел загроз інформаційній безпеці. При цьому саме поняття кінцевої станції істотно розширилося за останні роки, особливо з розвитком мобільних платформ. Тепер в область визначення «кінцевої станції» входять не тільки персональні комп'ютери користувачів і корпоративні сервери, але і мобільні пристрої (смартфони, планшети, ноутбуки) і пристрої IoT (Internet of Things). З цієї ж причини значно збільшилася кількість векторів атак, як на корпоративні мережі, так і на простих користувачів.

Стрімкий розвиток концепції BYOD (Bring Your Own Device) в середині 2000-х років вніс свої корективи в розмивання периметра організацій і збільшення векторів атак. Якщо раніше смартфони, домашні комп'ютери і ноутбуки користувачів не представляли великого комерційного інтересу для зловмисників, то з перенесенням на них частини корпоративних функцій вони стали вельми бажаними цілями для атак.

Лавиноподібне збільшення спрямованих атак в 2010-х роках, відмінною рисою яких є експлуатація вразливостей нульового дня, унеможливило для використання класичний підхід до захисту кінцевих станцій, пов'язаний виключно з сигнатурним і статичним аналізом запускаються файлів.

Останнім часом йде збільшення спрямованих атак на кінцеві станції, що реалізуються за допомогою т.зв. fileless malware, що зберігаються виключно в оперативній пам'яті і не залишають записи про свої активності в файловій системі. В цьому випадку з архітектури атаки повністю зникає головний об'єкт перевірки класичного антивіруса - сам заражений файл.

1 АНАЛІЗ СУЧАСНИХ ЗАВДАНЬ ТА ВИМОГ ДО ПРОДУКТІВ ENDPOINT PROTECTION PLATFORM

1.1. Роль Endpoint Protection Platform у інформаційній безпеці

Піонерами в захисті кінцевих станцій, безумовно, були антивіруси, історія яких починається з середини 80-х років минулого століття. Основою будь-якого антивіруса завжди був сигнатурний аналіз - технологія, що дозволяє по деякому принципом обчислювати контрольну суму зараженого файлу і записувати її в централізовану сигнатурну базу. При подальшій перевірці кожного проходить файлу його контрольна сума порівнюється з усіма записами в сигнатурної базі і при збігу файл позначається як заражений. Очевидним недоліком такого методу є те, що з його допомогою можна виявити лише ту загрозу, інформація про яку вже є в базі - нові уразливості і методи їх експлуатації випадають з поля зору сигнатурного аналізу.

Наступним логічним кроком у розвитку антивірусних систем став статичний (або, як його частіше називають, евристичний) аналіз. Суть статичного методу полягає в тому, що на базі певного набору патернів і статичних ознак (властивостей) евристичний механізм намагається передбачити поведінку аналізованого файлу до того, як той зможе завдати шкоди системі. Незважаючи на те, що статичний аналіз в цілому збільшив відсоток виявлень шкідливих файлів (в тому числі відсутніх в сигнатурної базі), він також має низку недоліків. Основний з них - це обмеженість методу при ідентифікації атак, в яких, наприклад, експлуатуються невідомі уразливості в системному або прикладному програмному забезпеченні. В цьому випадку статичні властивості та інструкції, які використовуються зараженим файлом, з точки зору евристичного ядра можуть нічим не відрізнятися від інструкцій в легітимних файлах.

Не завжди основним вектором атаки є заражені виконувані файли. Дуже часто атаки на кінцеві станції йдуть через експлуатацію вразливостей в системному і прикладному програмному забезпеченні. Починаючи від атак на вразливості браузерів, коли користувач завантажує заражену веб-сторінку, і закінчуючи доставкою шкідливої корисного навантаження на кінцеву станцію через уразливості мережевих протоколів і операційних систем. В цьому випадку недостатньо просто перехоплювати і аналізувати заражений файл - необхідно забезпечувати захист мережевих з'єднань, аналізуючи мережевий трафік, що приходить і виходить з кінцевої станції. В рамках такого підходу до функціональності класичного антивіруса додаються технології мережевого захисту, такі як міжмережевий екран, система запобігання вторгнень і система контролю підключаються до кінцевої станції пристроїв.

Саме з цього моменту формується новий тип продуктів - платформа захисту кінцевих станцій, або Endpoint Protection Platform (EPP). Endpoint Protection Platform - це система комплексного захисту кінцевої станції, що включає в себе як класичну функціональність антивірусного захисту, так і розширені технології безпеки - персональні міжмережеві екрани, системи запобігання вторгнень, системи контролю портів і пристроїв, що підключаються, системи шифрування дисків та ін.

З певного моменту більшість EPP-рішень перестали задовольняти сучасним вимогам до безпеки кінцевих станцій. В першу чергу це було пов'язано з ростом спрямованих атак, які в основному використовують уразливості нульового дня і відрізняються масовістю завдяки використанню ботнетів і внутрішньої архітектури горизонтального поширення. Також необхідно відзначити окремий клас загроз - кріптолокеров (або шифрувальників), які в принципі, з точки зору системного програмного забезпечення, не роблять нічого протиправного. Відмінною рисою всіх цих атак є те, що вони не використовують відомі підходи і проломи, а експлуатують ще невідомі уразливості і способи свого поширення. Безумовно,

EPP-рішення були змушені еволюціонувати, щоб відповідати сучасним викликам в сфері захисту кінцевих станцій.

Підсумком такого еволюційного розвитку стала поява нових систем, об'єднаних під загальною назвою - NGEPP. NGEPP (Next Generation Endpoint Protection Platform) - це системи захисту кінцевих станцій, які крім базової функціональності класичного антивіруса, захисту мережі та контролю портів володіють розширеними функціями для боротьби з сучасними загрозами. Додатковими системами, що розширюють можливості класичних EPP-систем, можуть бути:

- Системи емуляції файлів у пісочниці (sandboxing) для боротьби з погрозами нульового дня.
- Системи Anti-Bot для боротьби з ботнетами, засновані на аналізі патернів трафіку і визначення в них бот-активності.
- EDR-системи (Endpoint Detect and Response) - системи реактивного захисту кінцевих станцій, що відповідають за розслідування інцидентів шкідливої активності і подальшого відновлення системи.
- Системи контролю додатків, які відповідають за блокування недовірених додатків (у тому числі на основі поведінкової аналітики), не дозволяючи останнім впливати на основні процеси та критичні дані.
- Системи захисту пам'яті, проактивно блокують підозрілу активність при зверненні додатків до оперативної пам'яті.
- Системи захисту даних, що включають в себе системи резервного копіювання, системи шифрування даних, системи запобігання витокам і системи боротьби з фішингом.

Gartner в своєму аналітичному звіті Redefining Endpoint Protection for 2017 and 2018 дає загальне визначення для Endpoint Protection Platform:

Рішення, розгорнуте на кінцевих пристроях, для запобігання атак на основі файлів, виявлення шкідливих дій і забезпечення розслідування і відповідної

реакції, необхідних для реагування на динамічні інциденти безпеки і попередження про них.

Таким чином, Gartner визначає, що EPP, як і класичний антивірус - це перш за все file-centric-система, яка відштовхується від припущення про те, що якщо не всі, то більшість атак на кінцеві станції проводяться саме через заражені файли.

При цьому сучасної EPP відводиться і роль EDR-системи з класичними ознаками таких систем - розслідування інциденту і можливістю формування реакції на нього. При цьому необхідно пам'ятати, що EDR-системи як клас з'явилися якраз з припущення, що неможливо запобігти 100% атак на кінцеві станції, і необхідності мати можливість досліджувати інцидент і виходячи з цього сформувати відповідну реакцію. Саме тому EDR в майбутньому повинен стати невід'ємною частиною будь-якого EPP-рішення, що претендує на звання Next Generation Endpoint Protection Platform.

Нарешті, динамічна реакція на інциденти і оповіщення про них - це також не нова функціональність, яка вже давно є прерогативою SIEM-систем, що мають свій об'ємний ринок.

Згідно з дослідженням Gartner (Magic Quadrant for Endpoint Protection Platforms 2018), останнім часом замовники віддають перевагу функціям захисту і виявлення в рамках EPP-рішення і не надають великого значення функціональності EPP, спрямованої на захист даних, наприклад, системам запобігання витоків або шифрування дисків і знімних носіїв. Також відмічено, що замовники, які купують рішення щодо захисту кінцевих станцій, все частіше задіюють вбудовані в операційну систему можливості захисту даних - такі, як BitLocker в Microsoft Windows 10 і FileVault в macOS. Одночасно з цим, захист серверів переходить від класичних EPP-рішень до спеціалізованих, сфокусованим на гібридних центрах обробки даних. В першу чергу це пов'язано з тим, що через розвиток віртуалізації, приватних і публічних хмарних платформ вимоги до безпеки серверної інфраструктури стали сильно відрізнятися від вимог до захисту кінцевих станцій.

Важливим зрушенням на ринку рішень по захисту кінцевих станцій є рух від реактивного захисту за допомогою IoC (Indicators of Compromise), які активно використовуються існуючими EPP-рішеннями (особливо з яскраво вираженою EDR-функціональністю), в сторону проактивного захисту за допомогою IoA (Indicators of Attack), використання яких дозволяє в реальному часі боротися зі складними спрямованими атаками. Безумовно, при русі від IoC-підходу, який близький до класичного сигнатурному аналізу, в сторону IoA-підходу виробники NGEPP використовують сучасні технології визначення атак, засновані в тому числі на технологіях поведінкової аналітики, машинного навчання і нейронних мережах.

Ще одною важливою відмінністю сучасних NGEPP є кількість підтримуваних платформ, починаючи від десктопних Windows і macOS, закінчуючи Open Source і мобільними рішеннями. Сьогодні в стандартні пакети практично будь-якого NGEPP-рішення включаються функції по управлінню безпекою мобільних пристроїв, які мають безліч перетинів з функціональністю спеціалізованих MDM-систем (Mobile Device Management).

Проте, обмежуючись таким широким визначенням EPP, можна випустити з уваги дійсно ефективні рішення для захисту кінцевих станцій, просто тому, що якийсь із перерахованих вище ознак ще не реалізований повною мірою. Тому в огляді пропонується усі EPP-системи розділити на три еволюційних класи:

1. Розвиток класичних антивірусних рішень
2. Розширення функціональності NGFW (Next Generation Firewall) на кінцевих станціяї користувачів
3. Окремі рішення, які використовують екзотичні та унікальні підходи до забезпечення безпеки кінцевих станцій

- Розвиток класичних антивірусних рішень

Цей клас EPP-рішень є прямим нащадком перших антивірусів. І якщо раніше антивірусні виробники боролися в основному за повноту і обсяг сигнатурних баз,

то сьогодні боротьба розгортається вже за зручність користування, вбудовані механізми самозахисту і стійкість до технікам обходу і новим загрозам.

Відмінною особливістю таких систем є наявність як корпоративних рішень з виділеної системою управління і звітності, так і рішень для захисту домашніх комп'ютерів користувачів і мобільних пристроїв, з підтримкою практично всієї Enterprise-функціональності.

До представників цього класу EPP-рішень можна віднести: Kaspersky Endpoint Security, TrendMicro Smart Protection Suites, ESET Endpoint Protection, Symantec Endpoint Protection, Dr.Web Enterprise Security Suite і ін.

- Розширення функціональності NGFW (Next Generation Firewall) на кінцевих станціях користувачів

В рамках комплексного підходу до забезпечення мережевої безпеки виробники NGFW були змушені створювати рішення для захисту кінцевих станцій, щоб забезпечити більшу видимість і не допустити розмиття периметра безпеки, особливо в організаціях, що використовують BYOD-підхід.

Маючи значний досвід в комплексній мережевої безпеки, виробники NGFW випускають досить конкурентні рішення, багато з яких по праву можна назвати NGEPP. Зазвичай рішення таких виробників представлені виключно в корпоративному сегменті.

До найвідоміших представників цього класу EPP-рішень можна віднести: Check Point Endpoint Security, Fortinet FortiClient, Palo Alto Networks Traps і ін.

- Окремі рішення, які використовують екзотичні та унікальні підходи до забезпечення безпеки кінцевих станцій

Класичний підхід інтеграції безлічі функцій захисту кінцевих станцій в одному продукті не завжди є єдино можливим. На доказ цього на ринку EPP стали з'являтися рішення, які виходять за рамки класичної парадигми захисту кінцевих станцій, але при цьому можуть скласти конкуренцію піонерам цього ринку.

Яскравим прикладом таких систем можна вважати CylancePROTECT, який використовує алгоритми машинного навчання для боротьби з відомими і невідомими погрозами, при цьому не вимагаючи регулярних оновлень і не використовуючи сигнатурний підхід. Ще один приклад нестандартного підходу - BufferZone, що відповідає тільки за контейнірованіе (запуск в ізольованому системному оточенні) всіх недовірених додатків, таким чином захищаючи системні файли і критичні дані без як такого аналізу активності додатків.

СНД ринок систем безпеки став відомий всьому світу багато в чому завдяки сильним рішенням в області захисту кінцевих станцій. Окремо варто виділити рішення «Лабораторії Касперського», які вже протягом багатьох років входять в світові лідери систем безпеки, пов'язаних не тільки із захистом кінцевих станцій. До сильних продуктів із захисту кінцевих станцій також можна віднести Dr.Web Security Space виробництва німецької компанії Dr.Web і Secret Net Studio виробництва компанії «Код Безпеки». «Код Безпеки» завжди був відомий продуктами для захисту даних від несанкціонованого доступу, що знайшло своє відображення і в їх комплексному рішенні. Із зарубіжних компаній окремо варто виділити ESET, яка стабільно потрапляє в трійку найпоширеніших EPP-рішень на нашому ринку. Необхідно відзначити, що продукти вітчизняних компаній, крім високого рівня захисту, мають широкий набір сертифікатів регулюючих органів, що дозволяє використовувати їх для захисту систем, які мають найвищі вимоги до захисту конфіденційної інформації та державної таємниці.

Турбота про захист внутрішньокорпоративних даних і побоювання щодо несанкціонованого витоку інформації більш ніж виправдані. Все частіше надбанням громадськості стають сенсаційні події, коли, наприклад, оприлюднюються конфіденційні відомості про клієнтів. Рішення для запобігання витоку даних і захисту кінцевих точок покликані вирішити цю проблему.

У багатьох виникає резонне питання, чи дійсно такі продукти здатні вирішити проблему або вони лише усувають окремі симптоми, як і раніше залишаючи надто багато прогалин в системі безпеки. В кінцевому підсумку йдеться

про дві групи завдань: по-перше, необхідно запобігти неправомірному і небажаному витоку інформації за межі підприємства, а по-друге, - мінімізувати ризики, пов'язані з використанням ноутбуків. Загальні підходи до вирішення поставлених завдань частково збігаються, тому запобігання витоку даних і захист кінцевих точок не так просто відокремити один від одного. Часто один продукт дозволяє хоча б частково охопити обидві області.

При більш пильному розгляді стає ясно, що запобігання витоку даних (Data Leakage Prevention, DLP) і захист кінцевих точок (Endpoint Security) - це лише окремі елементи великої теми «інформаційна безпека». Перш за все необхідно з'ясувати, як домогтися того, щоб лише певним користувачам (що знаходиться на території підприємства або за його межами) надавалася можливість доступу до певної інформації. При захисті кінцевих точок необхідно брати до уваги і класичні питання інформаційної безпеки - захист від вірусів і обмеження мережевого доступу (Network Access Protection).

Багатошаровість цієї теми проявляється також у тому, що класичні брандмауери, уніфіковане управління погрозами (Unified Thread Management, UTM) або управління правами доступу до інформації (Information Rights Management, IRM) теж націлені на захист систем і регулювання роботи з даними. Ті, хто близько знайомий з різними підходами, швидко переконуються в тому, що єдиного методу, за допомогою якого можна було б вирішити всі проблеми, не існує.

Ефективність брандмауерів обмежується наявністю безлічі різних комунікаційних шляхів. Для ноутбуків, USB-накопичувачів, мобільних телефонів і інших носіїв інформації централізований брандмауер не здатний перешкодити як виносу даних за межі компанії, так доставці вірусів і черв'яків всередину корпоративної мережі. Технологія IAM, в свою чергу, орієнтована насамперед на захист доступу до централізованих інформаційних ресурсів і систем. Це дозволяє запобігти звернення неуповноважених осіб до внутрішніх систем і зберігаються там конфіденційних даних. Але якщо доступ до даних надається особам з

належними правами, які згодом вирішуються використовувати інформацію неприпустимим чином, то технології IAM виявляються безсилі.

Технологія IRM захищає безпосередньо інформацію, але її краще всього використовувати за межами підприємства. Однак, оскільки основний акцент робиться на документах, бази даних залишаються без захисту, і гучні інциденти, коли у відкритому доступі виявилися великі обсяги відомостей про клієнтів, не вдалося б запобігти.

Досить важко провести різницю між зберіганими даними (data at rest), даними що передається (data in move) і даними, що використовуються на робочих станціях (data in use). Необхідно, щоб захист здійснювався в будь-який момент часу. Так, підхід, при якому інформація, наприклад, шифрується на локальному жорсткому диску комп'ютера, але без додаткового захисту копіюється на інші системи або пересилається по електронній пошті, зачіпає лише одну область.

Критична важливість переходів між цими фазами проявляється у багатьох сферах. Так, якщо електронні листи передаються по мережі в незашифрованому вигляді, то захист поштових скриньок на сервері електронної пошти виявиться малоефективним. Ще один актуальний приклад - інформація про кредитні картки: тут загрозу безпеці представляє так званий процесор, тобто інстанція, де здійснюється обробка транзакцій. Після того як захищені дані (data at rest, data in move) надходять в обробку (data in use), засоби безпеки вже не діють.

Очевидно, що точкові рішення лише частково справляються з ситуацією, оскільки підприємства не контролюють «фазові переходи», а часом і цілі етапи використання інформації.

Адміністрування директив у вирішенні Novell Zenworks Endpoint Security Management (ZESM) здійснюється через простий у зверненні інтерфейс Windows.Тем Проте ринок рішень для запобігання витоку даних існує і росте, а подібні інструменти мають право на існування. Однак їх слід розглядати в контексті комплексної концепції безпеки, про що ми ще поговоримо докладніше.

Ринок таких інструментів дуже неоднорідний: він ділиться на системи на базі мережі і на базі хостів. Перші намагаються вирішити задачу на рівні мережі, проте це тягне за собою проблеми, аналогічні вже згаданим в зв'язку з брандмауерами: якщо користувач працює зі своїм ноутбуком за межами локальної мережі підприємства, то від систем на базі мережі так само мало користі, як і в разі копіювання даних на носій USB.

Що ж стосується систем на базі хостів, то вони виконуються на самих клієнтів. Деякі функції навіть інтегровані в операційні системи Windows. Групові директиви в Windows (починаючи, головним чином, з Windows Vista) пропонують досить різноманітні адміністративні можливості для захисту від витоку інформації. Наприклад, можна задавати типи пристроїв USB, що застосовуються користувачами. Типові методи - контроль і обмеження використання пристроїв USB або настройка параметрів, що визначають, які типи даних і вмісту можуть копіюватися на зовнішні інформаційні носії. У цю групу, крім іншого, входять рішення для автоматичного шифрування вмісту на зовнішніх носіях, а також - в ширшому сенсі - спеціальні USB-носії, автоматично виконують шифрування і дозволяють доступ, наприклад після біометричної аутентифікації за допомогою вбудованого сканера відбитків пальців.

Ефективне використання таких підходів має на увазі централізоване адміністрування, як, зокрема, це реалізовано в групових директивах Windows. Однак лише деякі з пропонованих інструментів придатні для інтеграції в групові директиви. Найчастіше інтерфейсів для централізованого адміністрування виявляється недостатньо, і навіть якщо вони є, то мова, як правило, йде про нестандартні підходи.

Концепція Endpoint Security простягається за межі технологій DLP. Її завдання - захист кінцевих пристроїв, куди в якості підфункції входить захист від неуповноваженого вилучення інформації з кінцевих пристроїв.

У цьому випадку мова йде і про локально встановлене програмне забезпечення в комбінації з централізованим інтерфейсом адміністрування. Такі рішення мають безліч функцій, в тому числі наступні:

- антивірусна функція і захист від фішингу;
- індивідуальний брандмауер;
- виявлення та запобігання вторгнень;
- захист бездротових мереж (Wireless Security);
- шифрування даних на рівні жорстких дисків, папок і файлів;
- шифрування на зовнішніх пристроях і в середовищах зберігання;
- захист від копіювання певних типів файлів і їх місти-мого;
- контроль трафіку FTP;
- контроль мережевого доступу (Network Access Control, NAC);
- контроль USB-накопичувачів і інших пристроїв.

Однак представлені на ринку інструменти, як правило, не підтримують відразу всі функції. У деяких випадках пропонується розширити функціонал за допомогою додаткових продуктів того ж виробника, хоча їх вартість і зусилля по впровадженню та адміністрування можуть виявитися занадто обтяжливими.

Користувачі часто впираються в межі можливостей захисту - наприклад, якщо вам потрібно встановити USB-карт UMTS їх застосування доводиться дозволити. Однак ці пристрої, як правило, володіють власними ресурсами зберігання і можуть використовуватися для переміщення конфіденційних даних. Спроба обмежити дозволені типи файлів теж приречена на невдачу. Так, підприємство може заблокувати файли форматів XLS і CSV, але що завадить співробітнику скопіювати потрібну інформацію у вигляді документа Word або, витративши більше часу, як файл PPT? Такі дії проконтролювати не вдасться.

Ще один виклик - мобільність. Питання про те, в якому обсязі діють правила безпеки, коли пристрої використовуються за межами внутрішньокорпоративної мережі, при багатьох підходах до сих пір не вирішено остаточно. Мова йде не

тільки про ноутбуках. Більшість сучасних мобільних телефонів в стані синхронізувати дані і зберігати великі обсяги інформації.

А ось рівень адміністрування цих пристроїв і концепції їх захисту можна порівняти зі станом справ для ПК станом на кінець 80-х років.

Як і в інших продуктах, в Sophos можна вибирати компоненти для подальшого встановлення. Рішення DLP і концепції захисту кінцевих точок здатні знизити ризики безпеки. Однак користувачам необхідно розуміти, що з їх допомогою вони зможуть залатати деякі прогалини, але залишиться безліч інших потенційно небезпечних місць. Запобігання витоку даних і захист кінцевих точок повинні представлятися не тактичними точковими рішеннями, а елементами цілісної концепції безпеки IT, в яку - з метою зниження ризиків для безпеки - включаються і інші тематичні блоки, такі як брандмауери, UTM, системи управління подіями інформаційної безпеки (Security Information and Event Management, SIEM), IAM і IRM.

З одного боку, це передбачає чітке усвідомлення загроз IT, аж до повної оцінки ризиків; з іншого, вимагає наявності стратегії безпеки, в тому числі стратегії авторизації, де концепції безпеки та доступу до систем та інформації розглядалися б як єдине ціле. Без таких стратегічних підходів користувачі приречені на постійне латання виникаючих дір замість того, щоб бути впевненими в досягненні дійсно високого рівня безпеки. Ризик помилкових інвестицій дуже високий, тому фінансування розробки стратегії безпеки і авторизації стає першочерговим завданням.

До того ж часто виявляється, що це лише незначні витрати в порівнянні хоча б з вартістю ліцензій для рішень Endpoint Security, які є лише одним з цеглинок у загальній концепції безпеки.

При виборі рішень для захисту кінцевих точок особливе значення мають такі аспекти:

- Повна функціональність. Багато рішень охоплюють лише частина необхідних функцій. Якщо виробники пропонують додаткові продукти, здатні заповнити наявні прогалини, слід приділити особливу увагу їх інтеграції.
- Ефективне розгортання. Клієнтські компоненти повинні легко поширюватися по мережі - навіть без використання спеціальних програмних рішень.
- Централізоване адміністрування. Адміністрування клієнтів повинно здійснюватися централізовано за допомогою директив, а також груп пристроїв і користувачів, щоб можна було ефективно управляти безліччю систем.
- Концепції безпеки. Інтерфейси адміністрування повинні мати у своєму розпорядженні потужної моделлю забезпечення безпеки, щоб самим не перетворитися в пролом в системі захисту.
- Інтеграція. Інтеграція з іншими підходами до безпеки IT - починаючи з IAM і SIEM і закінчуючи груповими директивами Windows - вкрай необхідна. Останнє особливо рекомендується для спрощення адміністрування.
- Підтримка платформ. Більшість сучасних рішень обмежуються лише найбільш поширеними версіями Windows. Інші операційні системи, особливо найбільш критичні в плані безпеки мобільні кінцеві пристрої, як правило, залишаються поза увагою.

На даний момент пропоновані на ринку продукти значно розрізняються за функціональними можливостями, тому підприємствам необхідно точно визначити, яке з пропонованих рішень буде відповідати їх вимогам в контексті загальної стратегії безпеки.

Згідно з визначенням експертів, захист від витоку даних (Data Leakage Prevention, Data Loss Prevention, DLP) - це автоматизований засіб для розпізнавання і / або блокування переміщення великого обсягу конфіденційних даних за межі

інформаційної системи по будь-яким використовуваним в повсякденній роботі каналам. У нашій країні системи DLP стали впізнаваним типом рішень для боротьби з витоками. Реалізації проектів по впровадженню подібних систем, що перешкоджають розкраданню конфіденційної інформації, сприяє зміна законодавчих вимог (зокрема, закон про захист персональних даних) і зростаюче розуміння важливості захисту цінних інформаційних ресурсів, що зберігаються в державних і комерційних організаціях. Російським замовникам доступні продукти DLP зарубіжних вендорів (Symantec, WebSense, RSA, McAfee, Trend Micro, Verdasys), а також російські розробки, з яких найбільш відомими є рішення InfoWatch.

Як стверджує Рустем Хайретдінов, заступник генерального директора InfoWatch, системи DLP в класичному розумінні слабо затребувані навіть на американському ринку, де і виникло це поняття. На відміну від рішень щодо захисту інфраструктури (антивірусів, міжмережевих екранів, засобів захисту від спаму і т.п.), Впровадження систем DLP - досить трудомістка процедура, для успіху якої потрібно звернення до консалтингових послуг. Крім того, віддачу від впровадження складно виміряти, тому світовий ринок «чистих» продуктів DLP стагнує, а в Росії, по суті, він і не почав розвиватися. Наприклад, продукти DLP компанії InfoWatch більшість клієнтів використовують не для запобігання витоків, а для моніторингу звернень до конфіденційної інформації. Однак завдання захисту ніхто не відміняв, як би відповідний клас продуктів не називався і якими б різноманітними не були сценарії їх використання. Тому попит є, хоча і не такий великий, як прогнозували аналітики.

Дмитро Міхєєв, експерт центру інформаційної безпеки компанії «Інфосистеми Джет», вказує на наступну специфіку даного сегмента ринку. По-перше, в Росії сильні традиції тотального контролю в поєднанні з ігноруванням питань конфіденційності та доступу до особистої інформації. По-друге, витоки дійсно існують, і шкода від них значна як в плані фінансових втрат, так і загрози репутації. По-третє, цілий ряд регулюючих органів висуває вимоги до контролю

витоків - від PCI / DSS для компаній, що працюють з кредитними картами, до законодавчих актів про захист персональних даних. Зазначені обставини призводять до проблем, вирішити які неможливо без систем DLP. На цьому тлі все більш помітною стає тенденція до «взаємопроникнення» систем DLP, рішень для захисту робочих станцій (Endpoint Security) і контролю доступу (Network Access Control / Protection, NAC / NAP).

Останнім часом рішення для захисту робочих станцій стали включати в себе базові функції DLP - виявлення в переданих або копійованих файлах конфіденційної інформації за стандартними алгоритмами: атрибутам, ключовими словами і т.д. Тому можна говорити про взаємопроникнення технологій, що і підтверджує Рустем Хайретдінов. «Але клієнти, мені здається, поки не готові платити за ці функції, - застерігає Веніамін Левцов. - Купуючи продукт Endpoint Security, вони набувають в першу чергу антивірус, радіючи, що отримують додаткові інструменти. На жаль, неможливо побудувати скільки-небудь серйозну систему для боротьби з переміщенням конфіденційної інформації, використовуючи доступні в продукті Endpoint Security фрагменти DLP ». Що стосується NAC / NAP, то, на його думку, з часом такі системи будуть віднесені до класу систем, що забезпечують відповідність політикам і контролю IT (Compliance). Коли це трапиться, впровадження NAC буде здійснюватися як окремий проект в рамках глобальної програми впровадження проекту щодо забезпечення відповідності законодавчим вимогам.

За словами Рустема Хайретдінова, більшість рішень Endpoint Security випускається на базі відомих антивірусів. Як показує досвід InfoWatch, замовники перш за все обирають виробника антивіруса, а потім оцінюють інші засоби захисту. Наприклад, якщо постачальник Endpoint Security не випускає антивірусів, то продукти цього вендора найчастіше купуються, щоб доповнювати інші інфраструктурні рішення даного виробника.

Розглядаючи таке рішення, перш за все треба переконатися, що програма сумісна з бізнес-процесами, від яких залежить дохід компанії. Якщо засіб безпеки

перешкоджає основній діяльності, його просто не стануть використовувати в найбільш критичних точках інфраструктури, а, як правило, саме вони і є основними джерелами витоків. Далі слід проаналізувати вартість придбання і володіння, оскільки системи «на основі агентів» часто викликають чимало клопоту при впровадженні та експлуатації. Крім того, навіть найрозвиненіші рішення DLP і продукти для захисту кінцевих точок не здатні в повній мірі забезпечити безпеку внутрішньокорпоративних даних і вирішити проблему несанкціонованого витоку інформації. Те чи інше рішення вибирається залежно від «набору ризиків» і бюджету. «Система DLP - хороший інструмент для роботи з випадковими витоками або з витоками по стандартних каналах, - вважає Дмитро Міхєєв. - На такі витоки, за нашою оцінкою, припадає понад 85% подібних інцидентів, тому типові проблеми логічно вирішувати за допомогою готових інструментів».

Системи DLP розраховані, насамперед, на захист від дій безладних співробітників. З зловмисними інсайдерами справа йде складніше - тут потрібен комплекс організаційних і технічних заходів протидії, тоді і прогалин у захисті буде значно менше. Уже сьогодні більшість продуктів DLP інтегруються з іншими засобами захисту, системами проведення розслідувань, а також із засобами моніторингу інфраструктури, системами електронного документообігу, рішеннями щодо захисту контенту (DRM і шифрування). Деякі постачальники СЕД і UTM вбудували в свої рішення модулі DLP, ліцензуючи їх у відомих виробників. «Вважаю, що дана тенденція збережеться в найближчому майбутньому. Саме з цієї причини "Лабораторія Касперського" і InfoWatch планують розширення взаємовигідного співробітництва», - зазначає Рустем Хайретдінов.

За словами Веніаміна Левцова, продукти DLP є найважливішими постачальниками інформації для систем кореляції подій ІБ (SIEM), і часто їх впровадження ведеться в рамках суміжних проектів. «Але в інтеграцію з RMS / IRM-системами я не вірю, як і в майбутній розвиток систем розподілу прав на документи з використанням" контейнерного "шифрування. Основна причина - різке зростання навантаження на корпоративні служби підтримки і неможливість

утримувати рубрикатори конфіденційної інформації, які були б адекватними реальним потокам даних в великих середовищах. Наскільки я розумію, таких проектів одиниці, незважаючи на цілий ряд продуктових пропозицій від найбільших гравців».

«Навіть якщо технологія DLP буде інтегрована з іншими продуктами, вона не зникне, - вважає Дмитро Міхєєв. - Адже це не тільки технічні засоби, але і певна методика їх використання. Організувати запобігання витокам можна і без придбання виділеної системи DLP. Питання в тому, скільки сил і коштів зажадає така робота. Проблема безпеки - це проблема контролю діяльності людей. Поки в організації є хоча б дві людини, які займаються комерційною діяльністю, небезпека витоку існує. Які саме технології будуть застосовуватися для контролю, не дуже-то і важливо».

Бурхливий розвиток Інтернету призводить до того, що шкідлива активність поступово зміщує акценти з створення окремих черв'яків і вірусів, що атакують комп'ютери у випадковому порядку, до підготовленим цілеспрямованим атакам на корпоративні інформаційні системи. «Домашні» хакери-ентузіасти пішли в минуле, тепер на перший план виходять добре організовані і глобально розподілені кримінальні підприємства, основною метою яких є отримання доходу за рахунок складних незаконних фінансових схем.

Інформація, що надає певну цінність (наприклад, персональні дані, паролі, номери кредитних карт або стратегічні плани розвитку організації), розкрадається з різних місць. Потім ця інформація швидко реалізується на торгах через спеціальні координаційні центри і використовується зловмисниками в своїх цілях. Злочинні співтовариства регулярно підвищують кваліфікацію в прагненні збільшити розмір доходів, а збитки підприємств, які постраждали від хакерських атак ростуть, що призводить до проблем в бізнесі, втрати довіри клієнтів і посилення вимог з боку регулюючих органів.

Основним завданням служб інформаційної безпеки є захист корпоративних кінцевих точок, кількість яких може варіюватися від декількох десятків до декількох тисяч. В даному випадку під кінцевими точками розуміються всі пристрої, призначені для безпосередньої роботи користувачів - це настільні ПК, ноутбуки, планшети і смартфони. У спробі наздогнати постійно еволюціонують загрозами безпеці, співробітники IT відділів встановлюють на кінцеві точки безліч програмних агентів, як правило різних виробників. Такими агентами є антивіруси, хостової IPS, засоби управління пачтамі і додатками, системи шифрування і так далі. Кожен новий агент вимагає окремого сервера управління, політики безпеки, настроєний профіль, розкладу оновлень і попереднього тестування, що призводить до значного витрачання адміністративних і обчислювальних ресурсів організації. Крім того, одночасний запуск незалежних агентів може вплинути на стабільність роботи операційної системи і додатків.

З метою скорочення витрат з адміністрування та уніфікації механізмів захисту кінцевих точок ми рекомендуємо використовувати комплексні рішення з єдиним програмним модулем, який дозволяє об'єднати різні компоненти безпеки. При виборі виробника необхідно переконатися, що рішення відповідає вимогам стандартів безпеки, застосовує заходи безпеки більшості відомих загроз, прозоро для користувачів і має можливість централізованого управління.

Мережева безпека є найважливішою ланкою загальної системи безпеки організації, тому на неї виділяються значні кошти і ресурси. Захист корпоративної мережі організовується за рахунок комплексного, багаторівневого підходу, що охоплює всі потенційні уразливості. Цей підхід добре працює в контрольованому середовищі з високопродуктивними серверами і потужними програмними засобами аналізу трафіку. Кінцеві точки мають обмежені обчислювальні потужності, але при цьому часто містять важливі дані і конфіденційну інформацію, а також регулярно використовуються за межами захищеної корпоративної мережі. Тому нові реалії спонукають фахівців зосередити свою увагу саме на захисті робочої станції як потенційно уразливому ланці системи інформаційної безпеки.

1.2. Тенденції використання зловмисниками вразливостей кінцевих точок

Для того щоб обійти технологічні системи захисту периметра мережі, зловмисники концентрують зусилля на людському факторі - неуважність співробітників, що працюють на кінцевих точках.

Приклад 1: За допомогою фішинговою атаки користувач перенаправляється на заражений сайт, з якого відбувається прихована установка шкідливої програми (це може бути клавіатурний шпигун для збору конфіденційних даних, троян для організації бот-мережі або вірус для проникнення в корпоративну мережу).

Приклад 2: На територію організації підкидається флешка, яка містить шкідливі програми у вигляді файлів з нешкідливими, але цікавими назвами. Існує велика ймовірність, що співробітник, який знайшов флешку, спробує подивитися ці файли. Таким чином, шкідливе ПЗ потрапляє в корпоративну мережу в обхід всіх засобів захисту.

Корпоративними стандартами стають ноутбуки, планшети, комунікатори, тобто такі пристрої, можуть бути піддані небажаному впливу за межами захищеного периметра мережі організації. Найбільш гучні випадки витоку конфіденційних даних пов'язані саме з втратою / крадіжкою незахищених мобільних пристроїв і незашифрованих флешок.

Управління безпекою кінцевих точок являє собою складну проблему для IT-персоналу. Налаштування стандартної робочої станцій в організаціях з сотнями користувачів являє собою комбінацію з політик безпеки для різних агентів. Розгортання декількох видів програмного забезпечення, установка оновлень, підтримка політик і конфігурації в актуальному стані є досить трудомістким завданням, що неминуче призводить до помилок при налаштуванні параметрів безпеки.

Уразливості в стандартних мережевих протоколах дозволяють зловмисникам отримувати несанкціонований доступ до неконтрольованих або відкритим портам. А помилки програмування, нерегулярне оновлення операційних систем і додатків піддають кінцеві точки новому ряду атак і створюють службі безпеки додаткові проблеми.

На більшості підприємств розгорнуті продукти, спрямовані на рішення традиційних завдань безпеки - це антивіруси і, можливо, персональні брандмауери. Кожен раз, оновлюючи програмне забезпечення на кінцевих точках, інженери повинні зробити строгий цикл випробувань, щоб перевірити сумісність всіх клієнтських модулів.

Існують рішення, які дозволяють об'єднати функціональність захисту кінцевих точок в єдиному програмному агента для виконання всіх завдань безпеки. В результаті знімається навантаження з технічного відділу, так як потрібно тестування всього одного агента, знижуються витрати на розгортання клієнтських модулів, з'являється можливість перегляду параметрів безпеки за допомогою єдиного інтерфейсу управління. Крім того, користувачі робочих станцій виграють від більшої прозорості та розвантаженні системи. Важливою перевагою таких рішень є можливість віддаленого розгортання і установки агентів, а також централізоване управління політикою безпеки з єдиної консолі управління. Уніфікація технології безпеки кінцевих точок дозволяє спростити процес розгортання і управління функціоналом, призводить до зниження загальної вартості володіння засобами захисту. Для того щоб правильно вибрати рішення щодо захисту кінцевих точок і забезпечити мінімальний вплив на робочий процес, організаціям слід уважно вивчити продукти, представлені на ринку і визначитися з необхідним набором засобів безпеки.

1.3. Вимоги до комплексного захисту кінцевих пристроїв

Комплексний захист кінцевих точок повинен в себе включати:

1. Виявлення та блокування шкідливого програмного забезпечення

Виявлення та блокування шкідливих програм, націлених на кінцеві точки, традиційно входить в завдання окремих продуктів, таких як міжмережеві екрани, шлюзи Email і Web безпеки, антивіруси на робочих станціях. Міжмережеві екрани рівня додатків є необхідним компонентом мережевої інфраструктури будь-якої організації і здійснюють первинну обробку вхідного і вихідного корпоративного трафіку. Вони дозволяють блокувати небажаний шкідливий потік, визначають, які програми можуть отримувати доступ до мережі, роблять кінцеві точки невидимими для хакерів і фактично є першою лінією захисту периметра організації.

Антивірусні програми на робочих станціях призначені для запобігання проникнення вірусів безпосередньо на кінцеві точки. Практично будь-який сучасний антивірус використовує комбінацію методів виявлення шкідливого ПО на основі сигнатурного і евристичного аналізу. Сигнатурний аналіз здійснює перевірку файлів на наявність вірусів шляхом порівняння ділянок коду з сигнатурами з оновлюваної бази даних. Евристичний аналіз виявляє невідомі віруси шляхом зіставлення результатів емулюватися виконання програми і поведінкового коду відомих загроз. Додатковим функціоналом антивірусних програм може бути антишпигунський модуль, який зупиняє проникнення черв'яків, троянів, рекламного ПЗ та клавіатурних шпигунів на кінцеві точки. Він забезпечує захист в реальному часі від установки шпигунських програм, а також виявляє і видаляє програми, які були встановлені раніше.

При реалізації проектів з антивірусного захисту часто не беруться до уваги уразливості веб-браузерів. Кількість випадків фішингу та спеціальних Інтернет атак, таких як попутні завантаження, міжсайтовий скриптинг, шкідливі плагіни і доповнення браузера, неухильно зростає.

2. Шифрування даних на мобільних пристроях і знімних носіях

Крім крадіжки або втрати ноутбуків, заклопотаність викликають знімні пристрої зберігання даних: USB носії, карти пам'яті, CD і DVD-диски, які можуть містити великі обсяги інформації. Як тільки такий пристрій потрапить до чужих рук, відкриті дані відразу ж стають доступні для використання. Рішенням є впровадження повного шифрування жорстких дисків ноутбуків з передзавантажувальне аутентифікацией і шифрування знімних носіїв. Шифрування являє собою процес перетворення даних в закриту систему символів, які неможливо прочитати, нікому, крім тих, хто має ключ або пароль для розшифрування. Підтримка багатофакторної аутентифікації (смарт-карти, токени, біометрія) може забезпечити додатковий рівень безпеки. Раніше шифрування було складним громіздким процесом, завантажуються операційну систему робочої станції. Нові продукти щодо шифрування не мають таких проблем і встановлюються в глобальному масштабі на мільйони комп'ютерів.

3. Контроль доступу до портів введення / виводу

Різноманітність мобільних пристроїв, які можуть використовуватися в якості знімних носіїв і підключатися через порти введення / виводу робочих станцій значно ускладнює завдання захисту кінцевих точок від шкідливого ПО. До того ж безконтрольний доступ користувачів до мобільних пристроїв може призвести як до випадкової, так і до навмисної витоку конфіденційних даних. Штатні засоби, вбудовані в операційну систему, не дозволяють гнучко призначати права доступу користувачів до портів введення / виводу і контролювати переміщувану інформацію. Рішення з управління портами і пристроями, що підключаються до робочої станції, дозволяє підприємствам централізовано контролювати використання всіх знімних носіїв і мобільних пристроїв в мережі. Практичною перевагою є можливість блокувати несанкціоновану передачу важливих даних на знімний носій, а також виробляти примусове шифрування даних на носії, якщо вони задовольняють заданим критеріям.

4. Управління уразливими програмного забезпечення

На кінцевій точці може бути встановлено безліч додатків, як корпоративного, так і розважального характеру. Часто такі додатки, особливо найбільш поширені (Java, Skype, Adobe, Mozilla і т.д.) мають проломи безпеки, які можуть бути усунені тільки установкою відповідних пачтей і оновлень. Якщо централізоване оновлення операційних систем застосовується досить часто, то додатки оновлюються час від часу, що призводить до значних ризиків безпеки. На кожній кінцевій точці необхідно мати спеціальне програмне забезпечення, яке буде регулярно аналізувати всі наявні уразливості і своєчасно застосовувати до них патчі і оновлення.

5. Контроль запуску і цілісності додатків

IT персоналу необхідно контролювати, які програми запускаються користувачами під час роботи. Додатки можуть бути як небажаними (наприклад, розважального характеру або порушують ліцензійну політику), так і небезпечними (викачані з Інтернету і мають потенційну вразливість). Програмний агент, встановлений на кінцеву точку повинен вміти визначати, які програми дозволено запускати користувачеві, а які ні. Крім того, він повинен контролювати цілісність відповідальних додатків, особливо на важливих для організації системах (таких як банкомати, робочі місця бухгалтерів, термінали і т.д.).

6. Перевірка відповідності вимогам політик безпеки

Перед наданням логічного доступу в корпоративну мережу рекомендується застосовувати сканування кінцевої точки на наявність вірусів і перевіряти відповідність до основних положень політик безпеки. Вимоги політик можуть бути наступними: наявність останньої версії антивірусного програмного забезпечення і встановлених критичних патчів, відсутність запущених заборонених програм або гілок реєстру і т.д. При невиконанні будь-якого з цих вимог програмний агент повинен блокувати доступ пристрої до корпоративної мережі. Якщо співробітник

користується громадським комп'ютером, політика повинна перевіряти, щоб на машині не залишалася ніяких конфіденційних даних після такої сесії.

У складних корпоративних мережах необхідно враховувати в політиках безпеки роботу зі спеціальними шлюзами і системами аутентифікації різних виробників. Слід також підтримувати гостьовий доступ, а також автоматичне відновлення і установку оновлень на невідповідних політиці кінцевих точках. Деякі програмні модулі можуть здійснювати блокування або дозвіл доступу в мережу на основі серійного номера і моделі пристрою, а також сканувати знімні носії на наявність вірусів.

7. Безпечний віддалений доступ до корпоративної мережі

Поширеність мобільних пристроїв робить безпечний віддалений доступ необхідною вимогою для використання корпоративних ресурсів. Рішення полягає в установці агента віддаленого доступу, простоті надання з'єднання і надійної процедурі аутентифікації. Технологія віртуальних приватних мереж (VPN або SSL VPN) є найбільш поширеним засобом безпечного віддаленого доступу до мережі підприємства. Такий канал зв'язку захищає дані від перехоплення і фальсифікації шляхом встановлення безпечного зашифрованого тунелю між кінцевою точкою і центральним офісом. Деякі рішення щодо захисту мобільних пристроїв (на базі iOS, Android і Symbian) здатні надавати інформацію про фактичне місцезнаходження користувача за рахунок сигналу стільникового зв'язку. Безпека віддаленого доступу можна підвищити, застосовуючи многофакторную аутентифікацію на додаток до стандартного імені користувача та паролю.

8. Централізоване управління захистом кінцевих точок

Адміністратори повинні мати можливість централізованого управління засобами захисту кінцевих точок. Це дозволяє контролювати політики безпеки, планувати розкладу сканування і створювати звіти відразу для всіх робочих станцій організації. Крім того, важливою функціональною особливістю є можливість

віддаленого налаштування та розгортання клієнтів, відновлення паролів, блокування кінцевих точок.

Основні вимоги до рішень по захисту кінцевих точок:

- централізоване управління з можливістю поділу і делегування повноважень;
- моніторинг і звітність по кожному елементу управління кінцевою точкою;
- швидке виявлення, оповіщення та експертиза інцидентів безпеки;
- підтримка служб каталогів, таких як Active Directory і LDAP;
- комплексна звітність і підтримка аудиту на відповідність вимогам безпеки;
- швидке і просте розгортання програмних агентів, що не вимагає втручання користувачів;
- єдине управління подіями на кінцевих точках і в мережевому середовищі.

9. Прозорість для користувача

Програмний агент повинен впливати на діяльність кінцевого користувача тільки коли це необхідно відповідно до політики безпеки, або для попередження. Деякі рішення вимагають завантаження відразу всіх модулів агента на кожен комп'ютер, незалежно від використовуваних компонентів і придбаної ліцензії. В результаті "вхолосту" споживається значний обсяг ресурсів центрального процесора і оперативної пам'яті, що може привести до зниження продуктивності важливих бізнес-додатків. При виборі рішення необхідно враховувати співвідношення між легкістю управління, впливом на продуктивність і величиною втручання в роботу користувача. Гнучка конфігурація програмного модуля і установка на кінцеві точки тільки необхідних компонентів безпеки дозволяє поліпшити загальне враження користувачів, зменшити число звернень до служби підтримки і в цілому знизити вартість володіння рішенням.

10. Масштабованість і доступність

Рішення з безпеки кінцевих точок повинно мати можливість масштабироваться разом з ростом організації. Ручне видалення та перевстановлення агентів на кінцевих точках і серверах управління може порушити нормальні бізнес-процеси організації і привести до додаткових витрат. Легкість розгортання агентів на сотнях, тисячах або навіть десятки тисяч робочих місць може бути значною конкурентною перевагою при виборі рішення. Важливою вимогою до системи є локалізація і підтримка російської мови, що дозволяє користувачам нормально реагувати на повідомлення під час роботи програмного модуля.

Очевидно, що наявність одного антивіруса вже давно не забезпечує необхідний рівень захисту кінцевих точок від сучасних загроз інформаційній безпеці. Поширення мобільних пристроїв, збільшення ємності знімних носіїв, еволюція шкідливого ПО і нові типи атак вимагають застосування комплексного підходу до забезпечення конфіденційності даних і працездатності бізнес-додатків.

На даний момент на російському ринку представлена достатня кількість рішень по захисту кінцевих точок. При виборі продукту ми, перш за все, рекомендуємо звертати увагу на такі особливості як функціональність, сумісність з наявним ПЗ і сукупну вартість володіння. Досить часто виникають ситуації, коли «спокусившись» на невисоку початкову вартість продукту організація через деякий час змінює його на інший, більш дорогий, але і краще підходить для конкретної інформаційної інфраструктури.

2 ДОСЛІДЖЕННЯ КОНКУРЕНЦІЇ НА РИНКУ ENDPOINT PROTECTION PLATFORM ТА ВИЗНАЧЕННЯ ТЕНДЕНЦІЙ ІХ РОЗВИТКУ

2.1. Основні гравці на ринку Endpoint Protection Platform

У цьому розділі наведено короткий огляд продуктів Endpoint Protection Platform.

- Carbon Black Defense

Компанія Carbon Black була заснована в 2002 році і тоді називалася Bit9. У лютому 2014 року компанія Bit9 купила стартап Carbon Black, а 1 лютого 2016 року змінила назву з Bit9 на Carbon Black. У 2018 році компанія потрапила в квадрант візіонерів в аналітичному звіті Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій. У 2017 році в тесті NSS Labs в категорії Advanced Endpoint Protection (AEP) рішення Cb Defense єдине показало стовідсоткову ефективність у виявленні загроз і стовідсоткову стійкість до технікам обходу. Особливістю архітектури рішення, як і багатьох сучасних EPP-платформ, є т.зв. cloud-driven-підхід, при якому всі функції захисту реалізуються через легкий агент, який активно обмінюється інформацією з хмарної платформою. Консоль управління Cb Defence Окремо варто відзначити наявність спеціалізованого рішення Cb Protection для захисту критично важливої інфраструктури з вбудованими функціями аналізу програм, контролю звернень до пам'яті і контролю підключення пристроїв. Також рішення спрощує завдання відповідності вимогам до своїх достатків вбудованих звітів, метрик і рекомендацій з різних галузевим стандартам. Carbon Black має багате API і готові інтеграційні рішення з більш ніж 125 IT та ІБ-виробниками.

- Check Point Endpoint Security

Компанія Check Point заснована в Ізраїлі в 1993 році і протягом усієї своєї історії фокусувалася на комплексної мережевої безпеки. Є одним з лідерів в сегменті

NGFW (Next Generation Firewall). Логічним кроком стало розвиток окремого напрямку, пов'язаного із захистом кінцевих станцій, яке отримало назву Check Point Endpoint Security. До складу Endpoint-рішень входить кілька технологій: Threat Extraction і Threat Emulation - перевірка всіх скачуваних файлів в пісочниці Check Point SandBlast для захисту від загроз нульового дня. URL-Filtering, Zero Phishing і Credentials Protection - обмежує доступ до шкідливих або підробленими сайтам. Anti-Bot, Anti-Exploitation, Anti-Ransomware, Anti-Virus - технології, що дозволяють виявити і зупинити шкідливу активність Behavior Analysis Engine і Forensic Analysis - дозволяють автоматично усувати наслідки зупиненої атаки, в тому числі відновлювати зашифровані дані. Forensic Analysis - інструмент розслідування, що дозволяє автоматично встановити всі деталі атаки. Endpoint Data Protection - шифрування дисків і знімних носіїв (Media Encryption). Endpoint Access Control - поєднання міжмережевий екран, контролю додатків і VPN. Консоль управління Check Point Endpoint Management Server Відмінною рисою рішень Check Point Endpoint Security є одна з технологій емуляції проходять файлів, названа CPU Level Detection. У момент запуску перевіряється файлу пісочниця здатна відстежувати не тільки поведінку файлу всередині операційної системи, але і збирати діагностичну інформацію безпосередньо з CPU, дозволяючи тим самим визначати ще раніше не відомі експлойти.

- CylancePROTECT

Компанія Cylance була заснована в 2012 році і фокусується на захисті кінцевих станцій. У 2018 році компанія потрапила в квадрант візіонерів в аналітичному звіті Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій. Відмінною особливістю CylancePROTECT, флагманського продукту компанії, є те, що він не використовує класичні (сигнатурні, евристичні, поведінкові та т. Д.) Методи виявлення загроз, а спирається виключно на можливості штучного інтелекту в ідентифікації та блокуванні атак. Так само як і багато новатори в сегменті захисту кінцевих станцій, CylancePROTECT використовує архітектуру легкого агента, що не потребує щоденних оновлень, в

зв'язці з хмарної платформою, в якій реалізуються всі функції аналітики та управління. Консоль управління CylancePROTECT Варто відзначити, що будучи новачком на ринку EPP-рішень, Cylance посів третє місце в рейтингу Gartner Peer Insights Customer Choice Awards 2017 по результатам опитування замовників з корпоративного сектора з усього світу, поступившись лише рішенням Kaspersky Lab і Symantec.

- Dr.Web Enterprise Security Suite

Компанія «Доктор Веб» була заснована в Росії в 2003 році. При цьому розробка однойменного антивіруса і основного продукту компанії ведеться з 1992 року. Офіси компанії знаходяться в Росії, Казахстані, Україні, Німеччині, Франції, Японії та Китаї. На сьогоднішній день компанія «Доктор Веб» не приймає участі в порівняльних тестах міжнародних аналітичних компаній і тестових лабораторій. В рамках Dr.Web Enterprise Security Suite є кілька продуктів, які адмініструються через єдиний сервер управління. За типом захищаються кінцевих точок «Доктор Веб» виділяє кілька продуктів: Dr.Web Desktop Security Suite - рішення для захисту робочих станцій, клієнтів термінальних серверів, клієнтів віртуальних серверів і клієнтів вбудованих систем. Dr.Web Server Security Suite - рішення для захисту файлових серверів і серверів додатків (у тому числі віртуальних і термінальних серверів). Dr.Web Mail Security Suite - рішення для захисту поштових серверів на базі Unix, MS Exchange, Lotus (Windows / Linux), Kerio (Windows / Linux). Dr.Web Gateway Security Suite - рішення для захисту серверів виходу в інтернет на базі Kerio (Windows / Linux), Unix, Qbik WinGate, MIMEsweeper, Microsoft ISA Server і Forefront TMG. Dr.Web Mobile Security Suite - рішення для захисту мобільних пристроїв на базі Android і BlackBerry. Інтерфейс Dr.Web Desktop Security Suite Відмінною особливістю продуктів компанії «Доктор Веб» є система Dr.Web SpIDer Guard, яка на основі алгоритмів машинного навчання в повністю автоматичному режимі здатна визначати нові загрози і створювати нові правила детектування без участі вірусних аналітиків. Рішення «Доктор Веб» для захисту кінцевих станцій

знаходяться в Єдиному реєстрі вітчизняного ПО і мають сертифікати МО, ФСТЕК Росії і ФСБ.

- ESET Endpoint Protection

Компанія ESET зі штаб-квартирою в Братиславі (Словаччина) була заснована в 1992 році. В даний час продукти ESET можна більш ніж в 200 країнах світу, корпоративними клієнтами є понад 400 тис. Компаній. У різні роки в звітах Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій компанія потрапляла в квадранти нішевих гравців і візіонерів. В останньому звіті за 2018 рік компанія ESET стала єдиним виробником в квадраті претендентів (Challenger). Продукти ESET Endpoint Protection для систем Windows і macOS включають в себе два комплекти поставки - ESET Endpoint Antivirus і ESET Endpoint Security. Кожен з комплектів, крім основної функції антивірусного захисту, підтримує захист віртуальних середовищ, засоби для боротьби з фішингом і можливість віддаленого управління. У розширеному комплекті ESET Endpoint Security додаються технології обмеження веб-сайтів, двонаправлений міжмережевий екран і захист від ботнетів і спаму. Консоль управління ESET Remote Administrator З цікавих особливостей продуктів ESET Endpoint Protection варто відзначити наявність окремого шару контролю UEFI (у одного з перших на ринку), наявність внутрішньої пісочниці, HIPS-системи (Host-based Intrusion Prevention System), що відповідає за поведінковий аналіз додатків, а також унікальною (за заявами самої компанії) системи сканування пам'яті і системи захисту від мережевих атак.

- Falcon Endpoint Protection (CrowdStrike)

Компанія CrowdStrike була заснована в США в 2011 році і фокусується переважно на хмарних рішеннях для захисту кінцевих станцій. У 2018 році компанія потрапила в квадрант візіонерів в аналітичному звіті Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій. Рішення компанії Falcon Endpoint Protection об'єднує в собі рішення NGAV, EDR і MTH (Manage Threat Hunting). Примітна архітектура рішення, яка будується на двох сутності -

легковесном агента, що встановлюється на робочій станції і хмарної платформі, що відповідає за розширення функціональності агента за допомогою хмарних додатків (від NGAV до Threat Intelligence і Sandboxing), управління агентами і надання API для сторонньої інтеграції. Консоль управління CrowdStrike Falcon Відмінною рисою рішення, безумовно, є т. Н. cloud-delivered-підхід до захисту кінцевих станцій. Також варто окремо відзначити платформу CrowdStrike Threat Graph, яка відповідає за збір даних про атаки, їх збагачення з зовнішніх джерел і індикаторів компрометації (IoC), подальший аналіз із застосуванням технологій машинного навчання і поведінкової аналітики і створення індикаторів атак (IoA), які в подальшому поширюються на кінцеві станції. За рахунок такого підходу компанія значно знижує обсяг і частоту оновлень інформації на агентах, встановлених на кінцевих станціях.

- FortiClient (Fortinet)

Компанія Fortinet була заснована в США в 2000 році, фокусується на розробці рішень в сегменті NGFW і є одним з лідерів цього сегменту. FortiClient є логічним продовженням концепції комплексної інформаційної безпеки і доповнює основні продукти компанії. Основні компоненти рішення включають в себе: Antivirus, Anti-Exploit (Siganture-less-технологія визначення невідомих загроз), Sandbox Detection, Web Filtering, Application Firewall, IPSec і SSL VPN. FortiClient підтримує операційні системи сімейств Microsoft Windows, macOS, Linux, Chrome OS, iOS, і Android. Консоль управління FortiClient EMS (Enterprise Management Server) Цікавою особливістю FortiClient є можливість відправки в карантин заражених станцій з подальшою блокуванням будь-якої мережевої активності з цих станцій на всіх пристроях, що підтримують Fortinet Security Fabric.

- Kaspersky Endpoint Security

Компанія «Лабораторія Касперського» була заснована в Росії в 1997 році і протягом практично всієї своєї історії фокусувалася на захист кінцевих станцій. На сьогоднішній день компанія налічує 35 офісів в 31 країні світу. Регулярний учасник

рейтингів Gartner Magic Quadrant в категорії Endpoint Protection Platform - в 2017 році входила в квадрант лідерів, в 2018 - в квадраті візіонерів. Kaspersky Security для бізнесу - один з флагманських продуктів компанії, орієнтований на захист корпоративних кінцевих станцій, від SMB-сегмента до великих компаній. Kaspersky Security для бізнесу поставляється в декількох конфігураціях: Kaspersky Endpoint Security для бізнесу Стандартний - захист комп'ютерів, ноутбуків, мобільних пристроїв і файлових серверів. Контроль використання програм, пристроїв і інтернету. Захист від шифрування. Централізоване управління з єдиної консолі. Kaspersky Endpoint Security для бізнесу Розширений - інструменти рівня Стандартний, а також кошти системного адміністрування, шифрування даних, моніторинг вразливостей і автоматична установка виправлень. Kaspersky Total Security для бізнесу - інструменти рівня Розширений, а також захист поштових серверів, серверів спільної роботи і інтернет-шлюзів. Також варто відзначити рішення Kaspersky Endpoint Security Cloud, що включає в себе: хмарну консоль, захист комп'ютерів, ноутбуків і файлових серверів на базі Windows, macOS, мобільних пристроїв на базі iOS і Android і попередньо встановлені політики безпеки. Консоль управління Kaspersky Security Center Відмінною особливістю продуктів компанії «Лабораторії Касперського» є багаторівневий захист, що включає в себе: аналіз поведінки (Behavior Engine), захист від експлойтів (Exploit Prevention), «Анти-криптор» для захисту серверів від шифрування і власну репутаційну службу Kaspersky Security Network, яка отримує дані від більш 60 мільйонів вузлів по всьому світу. Рішення «Лабораторії Касперського» для захисту кінцевих станцій знаходяться в Єдиному реєстрі вітчизняного ПО і мають сертифікати ФСТЕК Росії і ФСБ Росії.

- Trend Micro Smart Protection Suites

Японська компанія Trend Micro була заснована в США в 1988 році, потім в 1992 році перенесла штаб-квартиру в Японію (Токіо). Компанія завжди була сфокусована на захист кінцевих станцій і безперервно потрапляє в квадрант лідерів Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій з самого

його появи в 2002 році. Продукти для захисту кінцевих станцій поставляються в двох комплектаціях: Smart Protection for Endpoints Suite і Smart Protection Complete Suite. Обидві комплектації включають в себе централізовану систему управління Trend Micro Control Manager і платформу для захисту кінцевих станцій, що включає всі компоненти, властиві NGEPP. У комплекті Smart Protection Complete Suite додатково передбачені можливості захисту поштових серверів, серверів спільної роботи і інтернет-шлюзів. Всі рішення доступні як для десктопних операційних систем (Windows, macOS, Linux), так і для мобільних платформ iOS, Android, Blackberry і Windows Mobile. Консоль управління Trend Micro Control Manager Відмінною особливістю рішень Trend Micro є те, що компанія однією з перших додала в свої продукти механізми високоточного машинного навчання, які включають аналіз файлів до і після запуску. Комплекс розширених технологій для визначення заражених файлів отримав назву XGen Endpoint Security і, крім машинного навчання, включає в себе технології контролю додатків, захисту від експлойтів і поведінкової аналітики.

- Symantec Endpoint Protection

Американська компанія Symantec є одним з лідерів ринку продуктів з інформаційної безпеки. Їх платформа для захисту кінцевих станцій Symantec Endpoint Protection не стала винятком - з 2002 року продукти компанії стабільно потрапляють в квадрант лідерів кожного Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій. Symantec Endpoint Protection являє собою інтегровану платформу щодо захисту кінцевих станцій, що включає в себе більшість систем, властивих NGEPP - починаючи з персонального брандмауера і закінчуючи системами EDR і sandboxing. Всі рішення доступні як для десктопних операційних систем (Windows, macOS, Linux), так і для мобільних платформ iOS і Android (SEP Mobile). Консоль управління Symantec Endpoint Protection Manager Відмінною особливістю продуктів компанії Symantec є набір signatureless-технологій визначення просунутих загроз: Advanced Machine Language (AML), що відповідає за розпізнавання невідомих загроз за допомогою механізмів машинного

навчання, Memory Exploit Mitigation, блокуючий експлуатацію вразливостей нульового дня , детектування атак за допомогою приманок (Deception) і система поведінкової аналітики Behavior Monitoring, яка проактивно блокує файли з підозрілою активністю.

- Traps (Palo Alto Networks)

Компанія Palo Alto Networks була заснована в США в 2005 році, фокусується на розробці рішень в сегменті NGFW і є одним з лідерів цього сегменту. У 2014 році компанія запустила свій продукт для захисту кінцевих станцій Traps. У 2017 році компанія потрапила в квадрант візіонерів в аналітичному звіті Gartner Magic Quadrant в категорії рішень для захисту кінцевих станцій. Traps архітектурно схожий з «новачками» ринку EPP - рішення складається з легкого агента для кінцевих станцій і хмарної платформи для аналізу загроз. Крім класичної функціональності EPP, в продукт вбудовані інші технології, такі як Machine Learning, захист від кріптолокеров, контроль запуску дочірніх процесів і блокування різних скриптів всередині документів. Крім цього, агент дозволяє відправляти файли на перевірку як в локальну, так і хмарну пісочницю Wildfire. Консоль управління Palo Alto Networks Endpoint Security Management (ESM) Відмінною рисою Traps є глибока інтеграція з пісочницею Palo Alto Networks WildFire і формування усіма замовниками глобальної бази індикаторів роботи шкідливого коду за допомогою алгоритмів машинного навчання і штучного інтелекту, за рахунок чого наповнюється аналітичне ядро Traps, а також поповнюється Threat Intelligence база на мережевій платформі NGFW.

2.2. Розвиток Symantec Endpoint Protection

За даними Datanyze, Symantec Endpoint Protection був другим за величиною продавцем на ринку систем безпеки кінцевих точок в 2019 році, поступаючись Trend Micro всього на один відсоток. Успіх цього програмного забезпечення

безпеки обумовлений масштабом корпорації Symantec і її великими інвестиціями в розвиток і маркетинг.

Стратегія ринку IT-безпеки різко змінилася за останні кілька років. Традиційні антивірусні і антивірусні продукти застаріли завдяки новим напрямкам атак, створеним хакерами усього світу. Проста перевірка процесів на комп'ютері по базі даних відомих вірусів більше не забезпечує достатнього захисту.

Symantec був одним з перших лідерів в антивірусної індустрії і щосили намагався випередити проблеми кібербезпеки. Продукти брандмауера для ринку житла стали менш прибутковими з моменту розширення використання домашніх маршрутизаторів Wi-Fi, які інтегрують міжмережеві екрани NAT. Включення безкоштовного Захисника Windows в свою операційну систему Microsoft виправила громадський інтерес до оплати за антивірусні системи. Symantec потрібно було знайти нові ринки безпеки, перш ніж вся його прибутковість зникла.

Корпорація Symantec працює з 1982 року. Компанії довелося повністю переглянути сімейство своїх продуктів на декількох етапах своєї історії і кожен раз уникати попадання на вмираючі ринки.

Symantec розкрила потенціал ПК в 1984 році і припинила випуск програмного забезпечення для мейнфреймів, повністю змістивши свою ринкову нішу з продуктів баз даних на системи генерування звітів. Аж до 1990 року компанія диверсифікувала свою продуктову базу, випускаючи утиліти для електронних таблиць, карти пам'яті для ПК і програму стиснення. Всі ці продукти були викинуті після того, як компанія придбала Peter Norton Software в 1990 році.

Symantec вже придбав антивірус, коли придбав сімейство продуктів Norton. Його система захисту була провідною антивірусною системою для MacOS. У Peter Norton Software також був різноманітний список продуктів, але тільки його антивірусна система.

Symantec запустив свій продукт Endpoint Protection в 2007 році. Вже усвідомивши, що до простих антивірусних систем більше не відносяться з повагою

в області кібербезпеки, компанії необхідно було розширити свої повноваження за допомогою більш складних систем для забезпечення безпеки бізнесу.

Антивірус все ще був в центрі Symantec Endpoint Protection, але пакет включав інші успадковані продукти в спробі зміцнити недоліки антивірусного підходу. Це був короткостроковий підхід «шок і трепет», щоб вразити потенційних клієнтів пакетом продуктів, який переважив пакети, пропоновані конкурентами. Це дало компанії час на перекодування всього антивірусного продукту, який вважався млявим, громіздким і займав занадто багато місця на диску. Урізаний код Endpoint Security займав п'яту частину дискового простору свого попередника., Symantec Corporate Edition 10.0.

Symantec Endpoint Security був скоріше маркетинговим тріумфом, ніж технологічним прогресом. Проте, читання ринку є найбільшою силою Symantec, і саме здатність ради директорів компанії визначати тенденції і їх готовність беззастережно об'єднувати продукти для нових підходів, зробили бізнес лідером на ринку.

Рада відзначила зростання числа керованих сервісів і випустив керовану версію Symantec Endpoint Protection в 2009 році. У 2010 році він випустив продукт, орієнтований на малі підприємства. У 2011 році він працював в зростаючій бізнес-тенденції хмарних сервісів і створив дружню для віртуалізації середу. Служба захисту кінцевих точок. Служба MSP і хмарна база даних сигнатур перетворилися в автоматизовану версію програмного забезпечення як послуги Symantec Endpoint Protection в 2016 році.

Незважаючи на майже щорічні зміни Symantec Endpoint Protection, система являла собою щось більше, ніж антивірусний пакет. За своєю суттю, продукт все ще використовував стару сервісну модель центральної дослідницької лабораторії, яка виявляла нові атаки і ідентифікувала сигнатури обробки. Потім ці підписи були розгорнуті в локальних базах підписів на клієнтських комп'ютерах, які надавали

вихідний матеріал для постійно діючої системи виявлення вірусів на кожному защищаемом пристрої.

Традиційні антивірусні методи вимагають центрального пулу експертів. Поширення оновлень бази даних загроз через Інтернет створює потенційну слабкість безпеки. Затримка між хакерами, винаходити новий вірус, і фахівцями в лабораторії, які виявили його, означає, що користувачі антивірусів завжди уразливі. Це особливо вірно, оскільки хакерської співтовариство реорганізовано в повністю керовані організації з власними конвеєрами продуктів.

По суті, Symantec Endpoint Protection працював на застарілій технології і покладався на маркетинговий відділ компанії. Тобто до версії 14, в якій був представлений AI.

Промислова балаканина вказувала на необхідність нових підходів до кібербезпеки з початку 2010 року. Дослідження в університетах США, Великобританії, Німеччини та Росії почали проникати в більш широкий світ за допомогою дослідних робіт і презентацій на конференціях з кібербезпеки і Symantec. вискочив на поле як шлях вперед або як мінімум, гарне маркетингове перевага.

Випуск Symantec Endpoint Protection 14 в листопаді 2016 достроково окупив себе. Це врятувало продукт від забуття новими постачальниками на ринку кібербезпеки, такими як Darktrace, Sophos і Fortinet. У той час як нові гравці в боротьбі були привабливіше, у Symantec був добре відомий бренд і дуже великий маркетинговий бюджет.

Symantec не завершила свою платформу штучного інтелекту, названу «Аналітика націлених атак» до 2018 року, але дегустація цієї тактики машинного навчання, яка була вбудована в Symantec Endpoint Protection 14, викликала велику увагу преси і тримала компанію на чолі ринку.

Symantec Endpoint Protection 14 є переломним моментом в стратегії кібербезпеки бізнесу. Інструмент об'єднує нові підходи до захисту кінцевих точок.

Традиційна модель дослідницької лабораторії, що відправляє поновлення бази даних загроз, перетворилася на гібридну локальну / хмарну конфігурацію. Інформаційний потік став двостороннім каналом.

Кожна установка - це дослідницький центр. Елемент програмного забезпечення машинного навчання виявляє загрози, аналізує попередні результати, виявляє нові віруси і ізолює їх. Потім він завантажує свої результати в центральну систему в хмарі. Потім це виявлення нової загрози поширюється по всіх інших установок Symantec Endpoint Protection по всьому світу. В даний час їх 175 мільйонів.

Ця архітектура являє собою майже однорангову (P2P) модель, яка застосовується для досліджень, яка представляє собою дуже практичне і ефективне використання ресурсів клієнта і постачальника. Велика різниця між цією комунікаційної архітектурою і P2P полягає в тому, що центральний сервер є посередником, що означає, що він все ще має слід традиційної моделі клієнт-сервер.

Локальне програмне забезпечення для Symantec Endpoint Protection встановлюється на хости, на яких виконується Windows, Macos, або Linux. Він має чотири основних види діяльності:

1. ідентифікація уразливості
2. запобігання атак
3. виявлення порушення
4. усунення загроз

Кожна з цих стратегій може звучати як нові імена для старих методів. Однак використання AI на кожному етапі означає, що операції виконуються з використанням методів, відмінних від використовуваних в традиційних AV-системах.

Зобов'язання системи захисту кінцевих точок по превентивних мірах включають в себе виявлення потенційних слабких місць безпеки в кінцевій точці.

Очевидні цілі тут включають USB-роз'єми, комунікаційні сервіси, комунікаційне програмне забезпечення, таке як браузери, і сервіси на комп'ютері, які потенційно можуть забезпечити точки входу для шкідливих програм.

Оцінка вразливості спрямована на зменшення поверхні атаки. Це безперервний процес, який встановлює і підтримує утиліти систем захисту від шкідливих програм, таких як простір пам'яті для пісочниці і карантину. Перевірка бази безпеки виявляє будь-які нові апаратні або програмні уразливості в міру їх додавання на пристрій.

Дії Symantec Endpoint Protection щодо запобігання атак прирівнюються до традиційної роботи брандмауерів. Метою тут є блокування попадання будь-яких нових вірусів в кінцеву точку. У новій методології програмне забезпечення Symantec блокує експлойти, які виявляють уразливості в програмному забезпеченні. Це також система управління виправленнями, тому що експлойти зазвичай закриваються виробниками програмного забезпечення з оновленнями.

Програмне забезпечення для запобігання атак захищає всі крапки входу в комп'ютер, включаючи мережеву карту і слоти USB.

Виявлення порушень є основним видом діяльності класичної антивірусної системи. У цій категорії завдань є елемент роботи брандмауера. Система виявлення порушень шукає кодові сигнатури, шаблони поведінки і послідовності активації програм для виявлення загроз. Це трохи більше, ніж класичний випадок перевірки бази даних сигнатур вірусів, оскільки він також перевіряє поводження. Це пов'язано з тим, що зловмисник може запустити довірене програмне забезпечення, вже встановлене в системі, для зловмисних цілей.

Система виявлення порушень запускає відповідь і реалізує блокування, зупиняє шкідливі процеси і направляє в карантин підозріле нове програмне забезпечення.

Після усунення безпосередньої загрози система Symantec Endpoint Protection запускає процеси для постійного блокування виявленої атаки. Ця фаза включає

звернення до Symantec Targeted Attack Analytics. TAA - це хмарний елемент системи захисту, і саме ця служба передає новини про атаку і її рішення іншим 175 мільйонам користувачів Symantec Endpoint Protection.

Процес виправлення відстежує запуски процесу, щоб визначити джерело на комп'ютері шкідливої стратегії. Він націлений на знищення будь-яких персистентних процесів, які спробують відновити будь-які знищені шкідливі дії на комп'ютері. Всі успішні спроби повертаються в TAA, щоб спільнота працюючих екземплярів також могло знищити набір шкідливих програм.

На етапі усунення загроз також присутній людський фактор. Технічні фахівці лабораторії в Symantec працюють зі звітами, шукаючи глобальні тенденції кіберзагроз, щоб вони могли краще адаптувати еволюцію програмного забезпечення Symantec Endpoint Protection.

2.3. Лідери на ринку Endpoint Security

Компанія OPSWAT, що спеціалізується на технологіях інформаційної безпеки, опублікувала рейтинг найбільших виробників антивірусного софту для Windows.

Лідером цього ринку названа компанія Symantec з часткою в розмірі 13,56%. В трійку ліденів також увійшли компанії Eset (12,84%) і McAfee (12,21%). «Лабораторія Касперського» розташувалася на п'ятому місці з результатом в 7,66%.

Судячи з оприлюднених даних, ринок антивірусів характеризується високим ступенем консолідації, при якій на ньому немає яскраво вираженого лідера з великим відривом від конкурентів. Таку картину можна бачити в усій ІБ-галузі, де на багатьох нішевих ринках (наприклад, міжмережеві екрани, VPN-сервіси, шлюзи електронної пошти) присутня велика лідируюча група, в якій немає абсолютно домінуючого гравця, зазначає портал ZDNet.

Високий рівень фрагментації є хорошим показником, оскільки різноманітна екосистема виробників - це очевидна ознака здорового і конкурентного ринку.

За словами експертів, ще однією ознакою здорового ринку є той факт, що він ніколи не стоїть на місці. Протягом багатьох років екосистема інструментів для захисту від шкідливих програм Windows постійно змінювалася. Змінювалися лідери: частки компаній то сильно падали, то істотно росли. Тому підтвердженням є зліт і падіння Avast за чотирирічний відрізок часу.

У початку 2014 року фахівці OPSWAT нарахували у Avast 13,2-процентну частку на глобальному ринку антивірусів, що було відчутно більше, ніж у найближчих переслідувачів. Через два роки частка компанії піднялася до 15%, а ще через такий же період - до 20,48%, чому значною мірою сприяло придбання AVG.

Екосистема інструментів для захисту від шкідливих програм Windows постійно змінюється

Однак згодом з невідомих причин Avast почала здавати позиції. До кінця 2018 року на компанію припадало 17,42% ринку антивірусних ПО, а в жовтні 2019 го показник опустився нижче 7%, і компанія опинилася на шостому місці в списку. Протягом 2019 року лідер на ринку змінювався тричі: спочатку їм стала McAfee, потім - Eset, потім - Symantec.

Дослідження OPSWAT також показує, що на антивірусному ринку ще є місце для інновацій і нових продуктів. Приклад - компанія Cylance, яка стала новачком у рейтингу і відразу зайняла сьому сходинку з майже 6-відсотковою часткою. Ривок Cylance пояснюють створенням рішень з використанням штучного інтелекту і предиктивної аналітики.

Експерти OPSWAT збирають інформацію більш ніж з 30 тис. Корпоративних і домашніх комп'ютерів, на яких встановлені антивіруси. У звіт не включається «Захисник Windows», оскільки він встановлений за замовчуванням практично на всіх сучасних системах Windows.

У OPSWAT відзначають, що звіт компанії не слід використовувати для визначення того, «які виробники засобів захисту від шкідливих програм є кращими або для порівняння цих постачальників з точки зору якості або продуктивності». Експерти рекомендують застосовувати ці дані лише в ознайомлювальних цілях.

3 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ТА ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ SYMANTEC ENDPOINT PROTECTION

3.1. Функціональні можливості Symantec Endpoint Protection

Symantec Endpoint Protection являє собою комплексне антивірусне програмне забезпечення, що включає в себе потужний фаєрвол. Призначений для роботи в корпоративному секторі, антивірус гарантує безпрецедентну захист від шкідливих програм і різних вторгнень.

Endpoint Protection від розробника Symantec - це унікальний у своєму роді продукт, здатний захистити не тільки від вірусів, але і мережевих погроз. Антивірус складається з декількох модулів і компонентів, чітко взаємопов'язаних між собою.

Не дивлячись на те, що комплекс створений для великих компаній, що володіють великою кількістю комп'ютерів, він цілком може використовуватися і в приватному порядку. Розробник потурбувався про забезпечення зручності користування користувачів і передбачив зрозумілий і простий інтерфейс, одну панель управління, як для фізичної, так і віртуальної платформи. Антивірус здатний працювати на будь-якій операційній системі Windows, Linux, Mac OS.

Одним з найважливіших вимог, які пред'являють користувачі до антивірусів, є їх швидкодія. Яким би відмінним не був антивірус, якщо він працює повільно, то значно ускладнює роботу користувачеві. Endpoint Protection в цьому плані вигідно відрізняється від своїх численних конкурентів.

Symantec Endpoint Protection - просте в налаштуванні і надійне в роботі комплексне антивірусне рішення з брандмауером, що пропонує посилений захист від усіх типів загроз і передбачає кілька рівнів безпеки

За допомогою технології машинного навчання в режимі поточного часу забезпечує превентивний захист і блокування спрямованих атак, а також підтримує віддалене розгортання і вибіркове застосування політик.

Symantec Endpoint Protection стане прекрасним рішенням для захисту віртуальних і хмарних дата-центрів в корпоративному середовищі.

Однак, використовувати антивірус можна і як некерований клієнт на будь-якому пристрої з ОС Віндовс, в тому числі і на домашньому комп'ютері або ноутбуці.

Програма представляє собою унікальне поєднання компонентів і інструментів:

- виявлення та усунення будь-яких типів вірусів;
- кілька видів сканування, в т.ч. за розкладом;
- запобігання і блокування вторгнень з мережі;
- варіативність правил проходження трафіку;
- контроль над додатками і пристроями;
- захист від експлуатації програмних вразливостей;
- моніторинг вхідної та вихідної пошти;
- емулятор для аналізу файлів в пісочниці;
- продумана система генерації звітів.

Підтримується розгортання захисного клієнта як в призначеному для користувача режимі роботи без централізованого управління, так і у вигляді мережевої структури із загальним сервером.

Продукт простий в інсталяції і має русифікований інтерфейс. Наявність якісної документації тільки спрощує процес знайомства з програмою. Легкому управлінню також сприяє і інтуїтивно зрозуміла навігація.

Будучи одним з кращих на ринку і зберігаючи лідерство в своєму сегменті, антивірус містить у собі універсальний набір можливостей:

- Протидіє різноманітним видам програмних загроз.
- Використовує передові інтелектуальні технології.
- Забезпечує швидкодію.
- Гарантує легке розгортання і гнучке управління.
- Має великий набір функціоналу.
- Щодня оновлює бази і сигнатури.

Symantec Endpoint Protection підтримує будь-яку збірку операційної системи від Microsoft, починаючи з ОС Windows 7.

Корпоративний комплексний антивірус Symantec Endpoint Protection

Роль антивіруса в житті корпорації або будь-який інший колективної мережі складно переоцінити. У міру прогресу технологій зростає і кількість недобросовісних програмістів, які вважають за краще вкрасти будь-які дані для своєї наживи, замість чесного заробітку.

Навіть, якщо ваша фірма не працює з електронними грошима, захист все одно потрібна, так як будь-яку викрадену інформацію зможуть використовувати проти вас зливаючи її конкурентам або шантажуючи. Існує й інший тип загроз, який навпаки вносить певну інформацію в систему з метою виведення її з ладу. Від усіх цих атак і не тільки, здатний захистити Symantec Endpoint Protection.

Цей корпоративний антивірус має найвищий рівень захисту і дозволяє не тільки боротися з погрозами, але результативно діє в превентивному варіанті, завдяки функції перевірки, аналізу репутації Insight. Вона здатна побороти хакерські атаки, які ще явно навіть не розгорнулися в вашій системі.

3.2. Технології захисту Symantec Endpoint Protection

Insight - це технологія, яка відстежує мільярди файлів на комп'ютерах клієнтів і в момент виникнення будь-якої загрози, про це повідомляється в

мережу. Сьогодні віруси працюють на основі технології швидкої мутації, таким чином блокуючи можливість антивірусів видаляти їх і виявляти в цілому. Основа роботи функції полягає в тому, щоб відстежувати мутуючі, зашифровані програми, тобто обернути перевагу шкідливого коду проти нього самого. У міру мутацій певних файлів система Insight підвищує рівень ризику для цього елемента, поки не дійде до критичного, тоді у всій мережі Symantec знатимуть про неякісне походження файлу. Технологія Insight підвищує частоту виявлення шкідливих файлів, збільшує продуктивність і точність всього антивіруса.

Insight являє собою сучасну функцію виявлення загроз, яка будується на підставі зібраної інформації з мільярдів файлів. Всі отримані дані дозволяють наносити точні і нищівні удари по відношенню до погроз.

Так як Insight виступає превентивної захистом, то SONAR - це захист в реальному часі.

Вбудована технологія SONAR забезпечує захист вже не на підставі контекстних даних, таких як оновлення, частота змін, виробник і т.д., а грунтуючись на характері роботи процесу. Простіше кажучи SONAR - це поведінковий захист.

Особливість функції полягає в тому, що навіть, якщо вірус зміг пройти через превентивний аналіз, він буде заблокований в реальному часі. Дуже важливо, що завдяки цій технології відбувається захист від атак нульового дня, а це ті віруси, які ще не були виявлені і переможені на світовому рівні. Таким чином, на захист від будь-якого шкідливого коду в стандартних програмах йдуть дні / тижні / місяці, тут же ви отримаєте підтримку своєчасно завдяки Symantec Endpoint Protection для Windows 10 або нижче.

Серед інших переваг Symantec Endpoint Protection варто відзначити хмарний сервіс антивірусного сканування (Intelligent Threat Cloud Service), просунуту технологію машинного навчання (Advanced Machine Learning - AML), поліпшує

статичну виявлення, функцію Generic Exploit Migration, що зупиняє атаки на клієнтські комп'ютери з Windows, і «пісочницю» для шкідливих програм.

Symantec Endpoint Protection це комплексне рішення для антивірусного захисту робочих станцій і серверів. Високий рівень безпеки і швидкодії, підтримка фізичних і віртуальних систем, без збільшення навантаження на системні ресурси системи

Швидко знаходить і видаляє шкідливий код на вашому сервері або робочої станції, такий як віруси, черв'яки, троянські коні, програми-шпигуни, руткіти, програми показу реклами, боти, а також невідомі раніше загрози (технологія Bloodhound).

Вбудований брандмауер дозволяє налаштувати фільтрацію вхідного трафіку через Інтернет або локальну мережу, блокує сканування портів і атаки хакерів, завантаження шкідливих програм на комп'ютер. Дозволяє зробити тонке налаштування параметрів мережевого трафіку.

Містить в собі нову революційну технологію Symantec Insight, що виконує превентивну захист від нових і швидко мінливих шкідливих програм, в тому числі раніше невідомих загроз, блокуючи їх роботу.

Має ручний і автоматичний режими сканування найбільш важливих областей і повне сканування всієї системи. Функції «Інтелектуального планувальника», для гнучкого налаштування часу проведення сканування системи.

Політика дозволяє контролювати запуск і роботу додатків на кінцевих пристроях користувачів. Підтримує налаштування правил за замовчуванням: зупинка інсталяції додатків, блокування запуску на знімних пристроях, доступу до скриптів і обмеження загального доступ до файлів, заборона зміни точок завантаження Windows і системних файлів і ін.

Підтримує роботу в системах Windows, Mac, встановлених як на фізичних, так і на віртуальних машинах. Інтеграція з провідними веб браузерами (Explorer, Mozilla, Firefox) для запобігання завантаження шкідливих програм і атак, спрямованих на уразливості браузерів. Автоматичний захист при роботі з електронною поштою в додатках Microsoft Outlook і Lotus.

Функція перевірки цілісності хоста дозволяє гарантувати захист клієнтських комп'ютерів за рахунок контролю виконання політик безпеки компанії. Політики дозволяють виявити порушення і примусово застосувати або відновити настройки безпеки на клієнтських пристроях для забезпечення безпеки корпоративних мереж і даних.

Локальна консоль адміністрування Symantec Endpoint Protection Manager або хмарна Integrated Cyber Defense Manager дозволяє централізовано керувати безпекою як локальних, так і віддалених комп'ютерів: настройка політик, розкладу оновлень, параметрів проксі-сервера. Можливість об'єднання користувачів в кілька груп з різним рівнем доступу для управління політиками, від повного доступу до блокування.

Автоматичне виявлення некерованих / незахищених пристроїв в мережі, деінсталяції стороннього антивірусного програмного забезпечення і оновлення клієнтів через LiveUpdate. Віддалена установка клієнта за допомогою локальної консолі управління Symantec Endpoint Protection Manager або створення інсталяційного файлу для інсталяції за допомогою сторонніх інструментів управління.

Забезпечення комплексної безпеки за рахунок інтеграції з Secure Web Gateway і ATP: Endpoint для захисту від спрямованих атак і складних загроз, за допомогою додавання в чорний список нових, раніше не відомих шкідливих програм, виявлених функцією контролю додатків.

Дозволяє при первинному скануванні нових файлів визначити і запам'ятати рівень їх надійності та ступінь уразливості. Надалі, при повторному скануванні,

використовуючи дані про репутацію цих файлів, технологія Insight пропустить надійні чисті файли (оскільки ступеня уразливості змінюються рідко). Рівень надійності ділиться на кілька категорій: файли, які є надійними з точки зору Symantec (категорія безпечніших), і файли, просканові і додані користувачами Symantec (категорія менш безпечних). Даний механізм дозволяє, не порушуючи загальної концепції безпеки, збільшити швидкість сканування систем.

Symantec Online Network for Advanced Response - технологія захисту в реальному часі. Виявляє потенційно шкідливі програми при їх запуску на комп'ютерах. Для виявлення нових і невідомих погроз SONAR використовує евристичний аналіз і накопичені дані про репутацію програм. SONAR надає захист "з нульовою затримкою", виявляючи загрози перш, ніж знадобляться стандартні інструменти виявлення вірусів і програм-шпигунів.

3.3. Компоненти клієнта Symantec Endpoint Protection

У головному вікні інтерфейсу клієнта Symantec Endpoint Protection для Windows показана актуальна інформація про стан захисту. Також для кожного компонента за допомогою кнопки Параметри можна перейти до відповідних настройки або в журнали їх роботи.

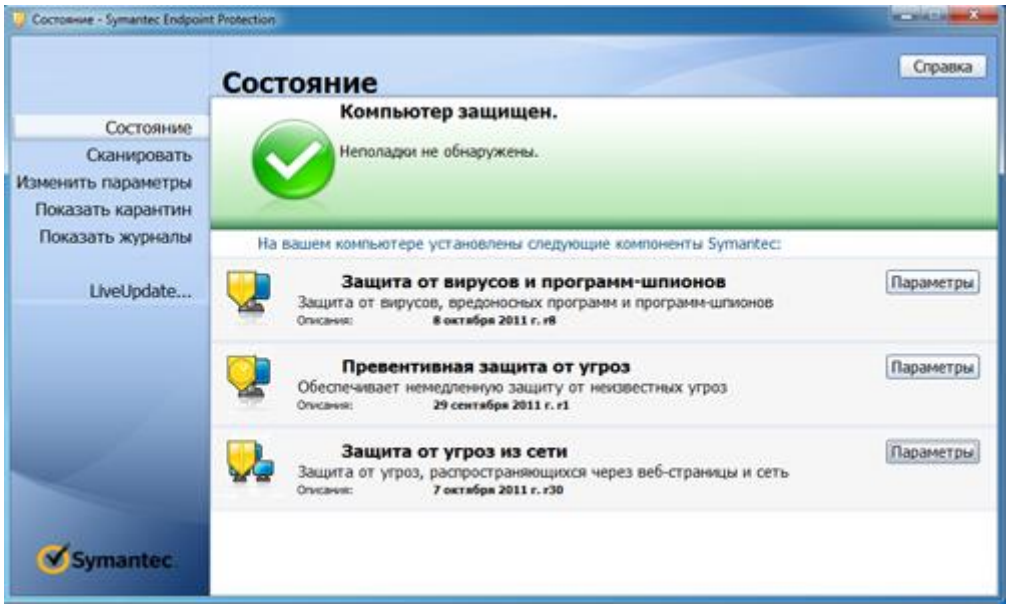

Рис.3.1. Головне вікно інтерфейсу в клієнті SymantecEndpointProtection

Якщо перейти в пункт меню «Сканувати» головного вікна інтерфейсу, то відобразяться завдання на періодичне сканування. Також доступні посилання на запуск активного сканування, або сканування всієї системи. При активному скануванні проводиться перевірка тільки деяких об'єктів файлової системи Windows, в яких найчастіше виявляються шкідливі програми. За допомогою переходу на відповідне посилання можна зробити глобальні настройки сканування.

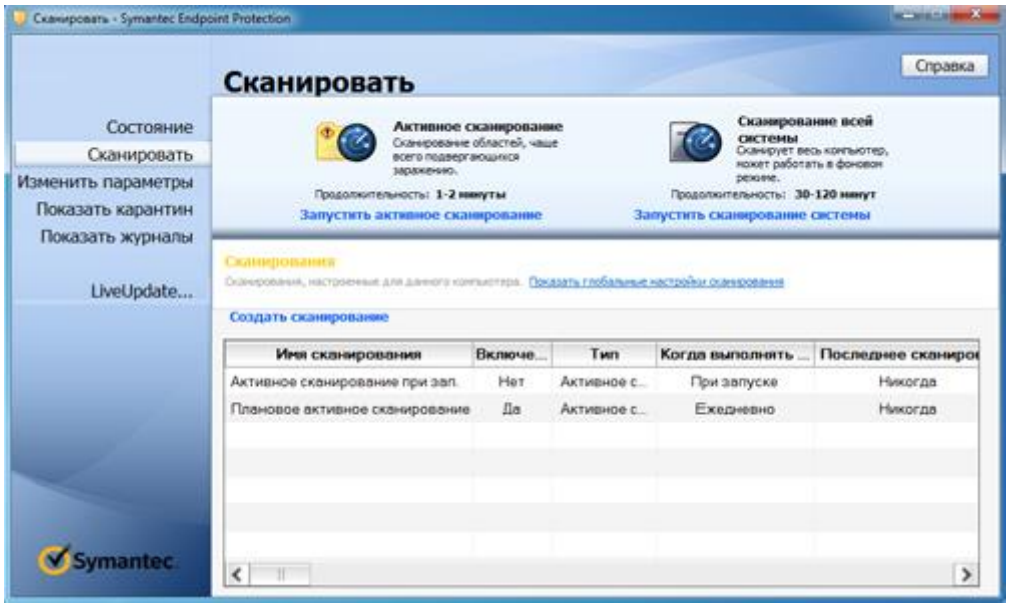

Рис.3.2. Пункт меню «Сканувати» в інтерфейсі SymantecEndpointProtection

При запуску сканування на вимогу відкривається вікно сканера, в якому відображаються хід та результати сканування, а також дії, вироблені з шкідливими об'єктами, ступінь ризику і тип виявлених загроз.

У пункті меню «Змінити параметри» головного вікна клієнта зосереджені налаштування всіх компонентів захисту Symantec Endpoint Protection 12 для Windows. Отримати до них доступ можна за допомогою кнопки «Налаштувати параметри», яка відображається праворуч від назви кожного компонента захисту.

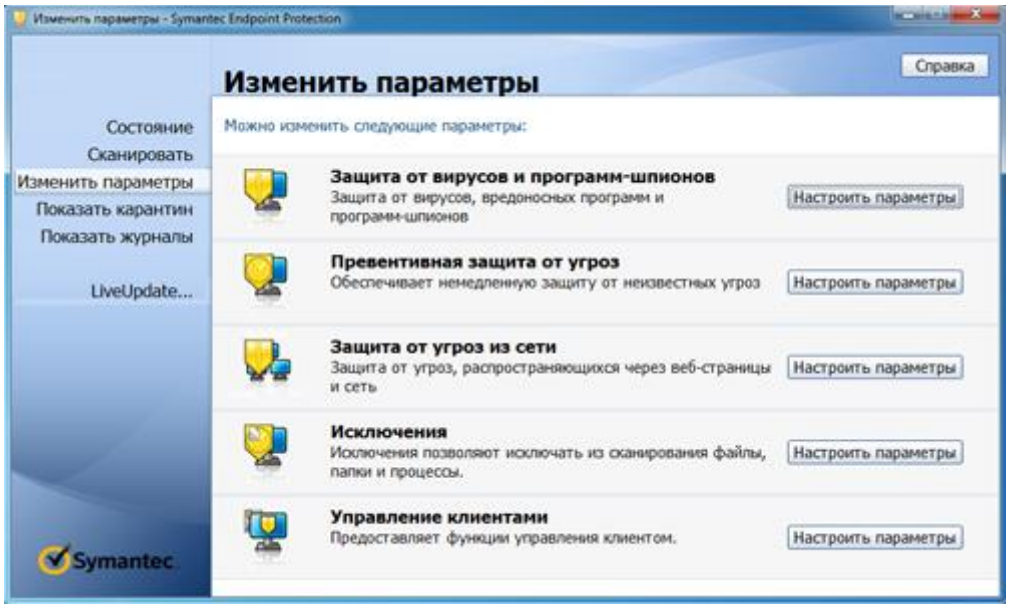

Рис.3.3. Меню «Змінити параметри» в інтерфейсі SymantecEndpointProtection

Вікно з параметрами роботи компонента «Захист від вірусів і програм-шпигунів» розбито на чотири вкладки: - Глобальні налаштування; - Автоматичний захист; - Download Insight; - Автоматичний захист інтернет-пошти. На вкладці «Глобальні налаштування» можна включити або відключити використання технологій Insight і Bloodhound. При цьому для технології Insight є можливість вибрати, яка саме інформація буде використовуватися для її роботи - тільки та, яка перевірена фахівцями Symantec або ж буде враховуватися інформація, яка надходить від спільноти користувачів продукту. Варіанти відрізняються один від одного рівнем впевненості в репутації файлів. У першому випадку рівень впевненості максимальний, але інформація існує про меншу

кількість файлів. У другому випадку є зовсім невелика частка ймовірності помилки, але кількість файлів, про які є інформація, максимальне.

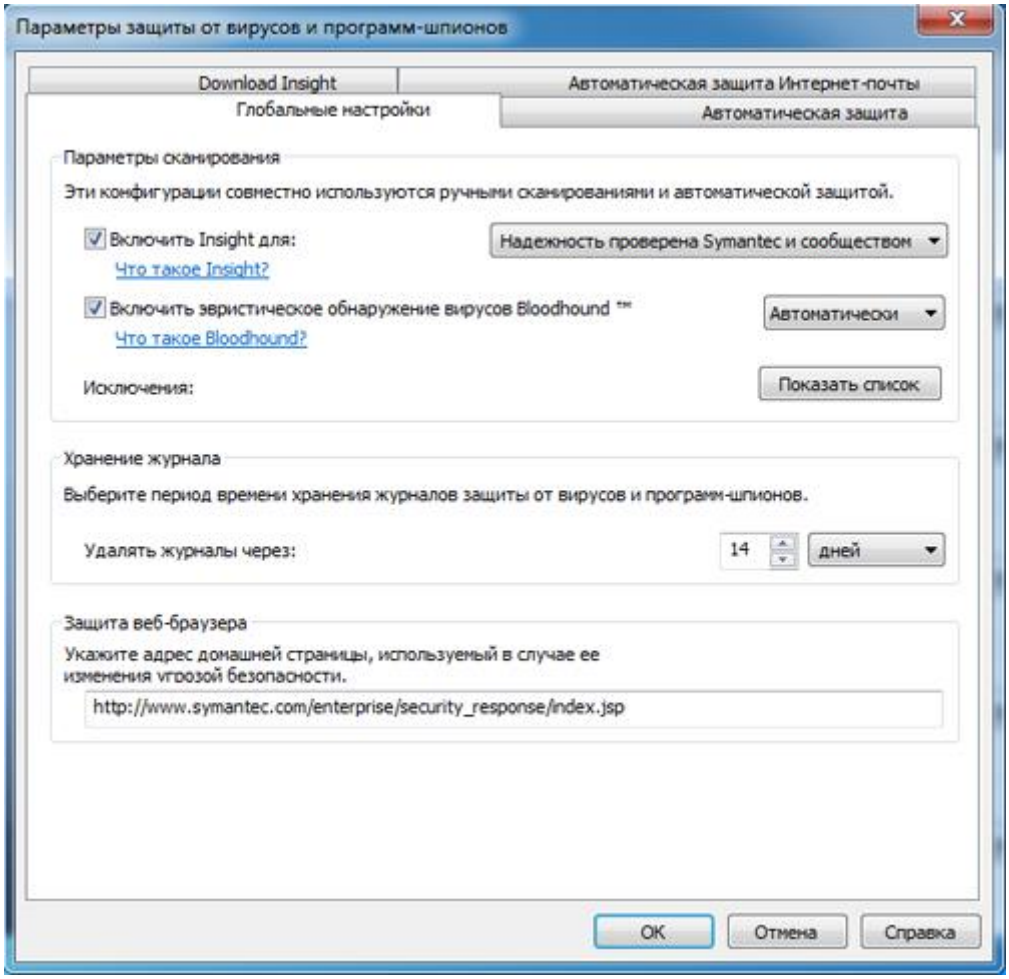

Рис.3.4. Вкладка «Глобальні налаштування» параметрів роботи компонента «Захист від вірусів і програм-шпигунів»

Репутаційна технологія Insight дозволяє пропускати при скануванні відомі безпечні файли. Технологія Bloodhound є проактивного технологією, яка ізолює деякі області файлів з метою виявлення значного числа невідомих шкідливих програм. У разі спроб проникнення програм за ізолюється периметр проводиться аналіз їх дій і приймається рішення про ступінь небезпеки цих програм. Вкладка «Автоматичний захист» присвячена включення і виключення сканування на наявність різних типів загроз. Також на цій вкладці можна налаштувати дії, які застосовуються до виявлених шкідливим файлів, налаштувати повідомлення,

налаштувати параметри перевірки дискет, а також задати параметри сканування, зібрані у вікні «Додаткові параметри автоматичного захисту».

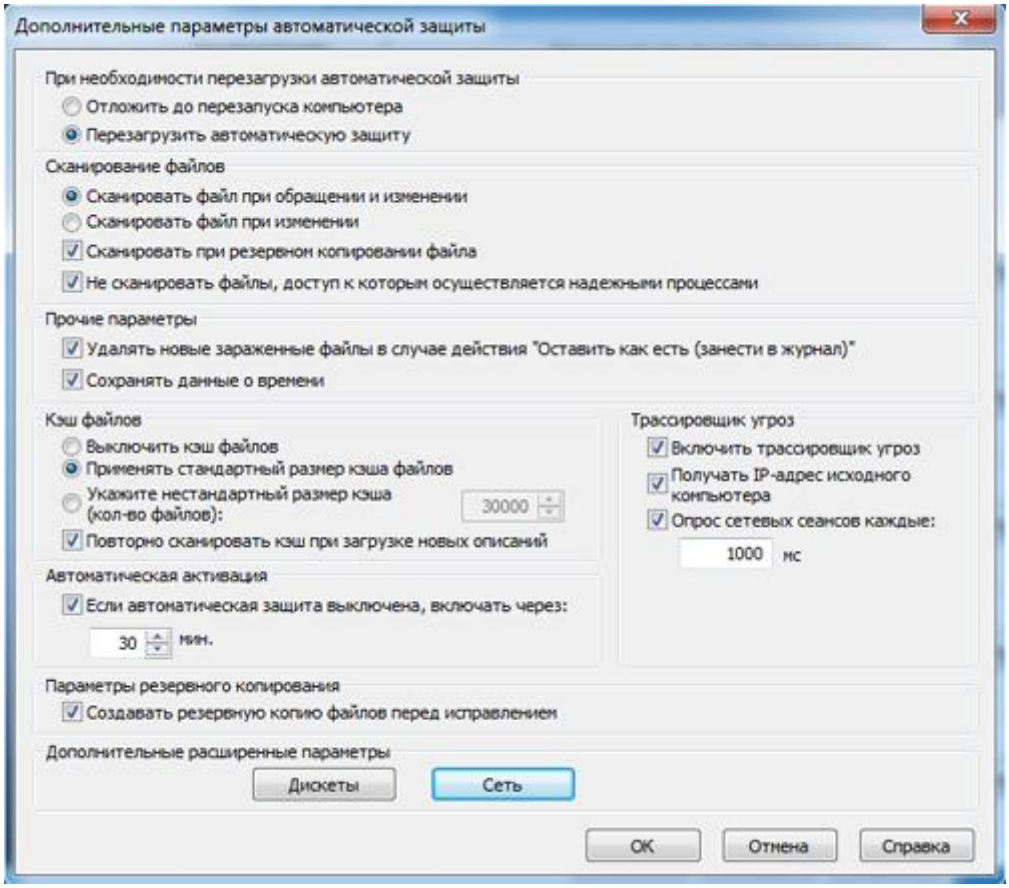

Рис.3.5. Додаткові можливості автоматичного захисту в Symantec Endpoint Protection

На вкладці Download Insight можна налаштувати роботу технології Insight при завантаженні файлів з Інтернету. Зокрема, можна задати чутливість роботи даної технології за 9-бальною шкалою, а також мінімальна кількість користувачів або мінімальний період «популярності» файлу для технології Insight перед прийняттям рішення. На вкладці «Автоматичний захист інтернет-пошти» можна, відповідно, налаштувати параметри перевірки поштового трафіку на захищається комп'ютері. Зокрема, можна налаштувати дії з листами, що містять шкідливі об'єкти і налаштувати відповідні повідомлення. Досвідчені користувачі можуть налаштувати роботу даного компонента більш тонко. Але в налаштуваннях є і обмеження. Зокрема, деякі хостинг-провайдери часто пропонують клієнтам використовувати нестандартний SMTP-порт, тоді як при відправці з інших ящиків

користувача може використовувати стандартний SMTP-порт. В налаштуваннях ж для перевіряється поштового трафіку в Symantec Endpoint Protection можна вказати лише один SMTP-порт. При цьому слід врахувати, що для клієнтів корпоративного антивірусного продукту це не настільки критично, як для домашніх користувачів.

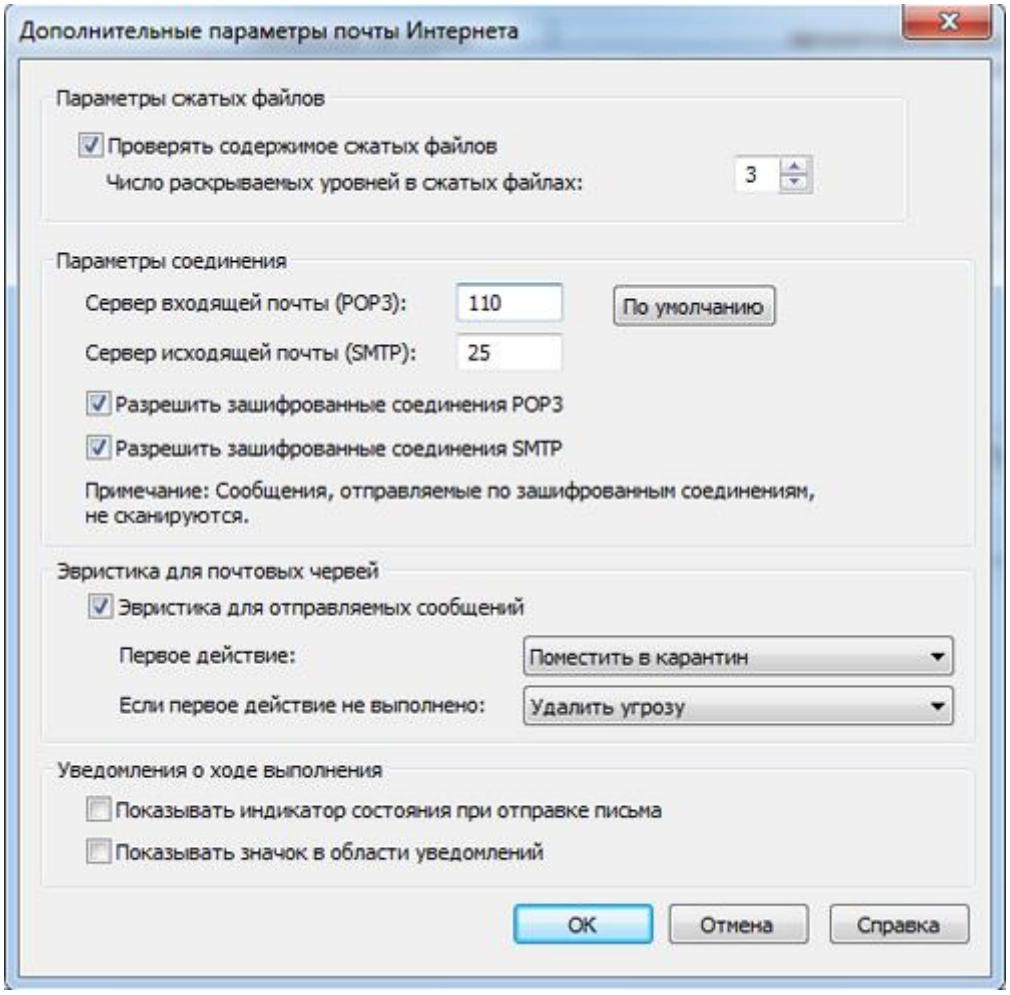

Рис.3.6. Додаткові параметри пошти Інтернету в SymantecEndpointProtection

Параметри «Превентивної захисту від загроз» розбиті на 3 вкладки:

- SONAR;
- Виявлення підозрілої поведінки;
- Виявлення зміни системи.

Перша вкладка присвячена налаштувань технології SONAR . Ця технологія поведінкового аналізу працює в режимі реального часу і виявляє потенційно

шкідливі програми при їх запуску або під час роботи. При цьому, для їх визначення використовуються як класичні евристичні технології, так і репутаційні, для реалізації яких функціонує глобальне хмара.

Дана хмарна репутаційна технологія, яка називається Insight, покликана виявляти нові і невідомі загрози, які неможливо виявити іншими способами, і одночасно економити обчислювальні ресурси системи (використання цієї технології, за інформацією вендора, дозволяє на 70% знизити навантаження на систему під час її сканування). На даний момент система містить анонімні дані про поширення більше 3 мільярдів файлів більш ніж на 175 мільйонах комп'ютерах клієнтів.

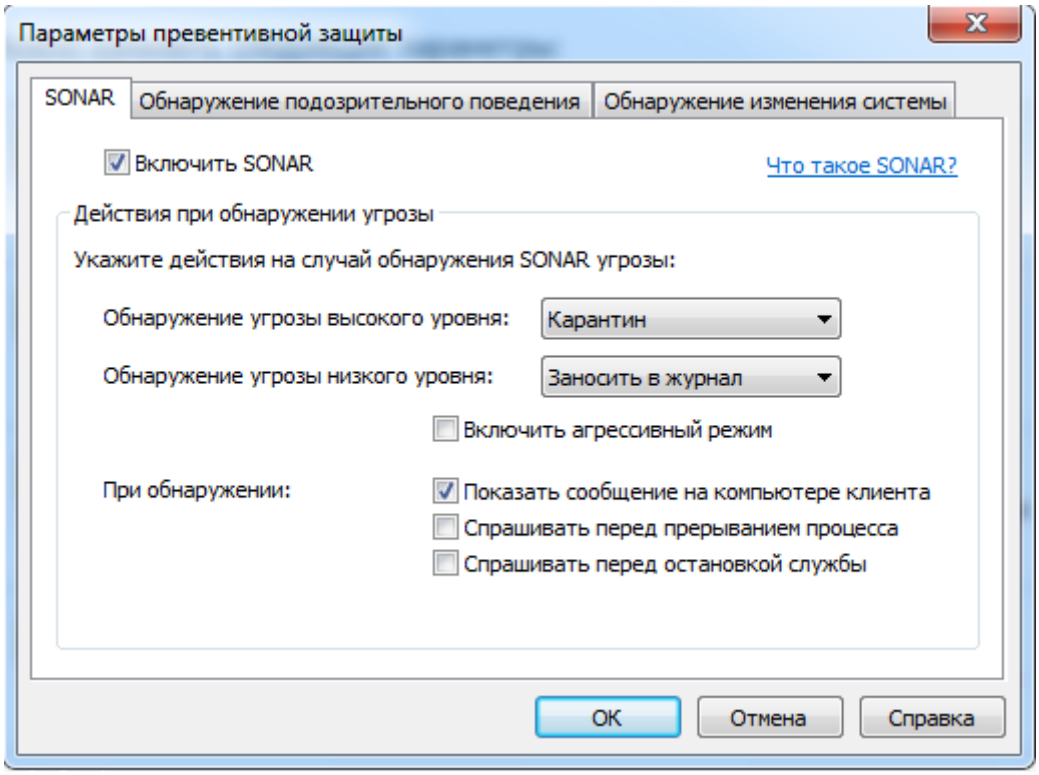

Рис.3.7. Параметри превентивного захисту в SymantecEndpointProtection

Дві наступні вкладки також призначені для налаштувань роботи технології SONAR. Перша відповідає за реакцію на погрози високого і низького рівнів, а друга відповідає за настройку реакції SONAR на змінення установок системи, таких як зміна DNS і файлу hosts. Налаштування для компонента «Захист від

загроз з мережі» розбиті на п'ять вкладок. Вкладка «Брандмауер» містить безліч параметрів, які дозволяють зробити базову настройку мережевого екрану.

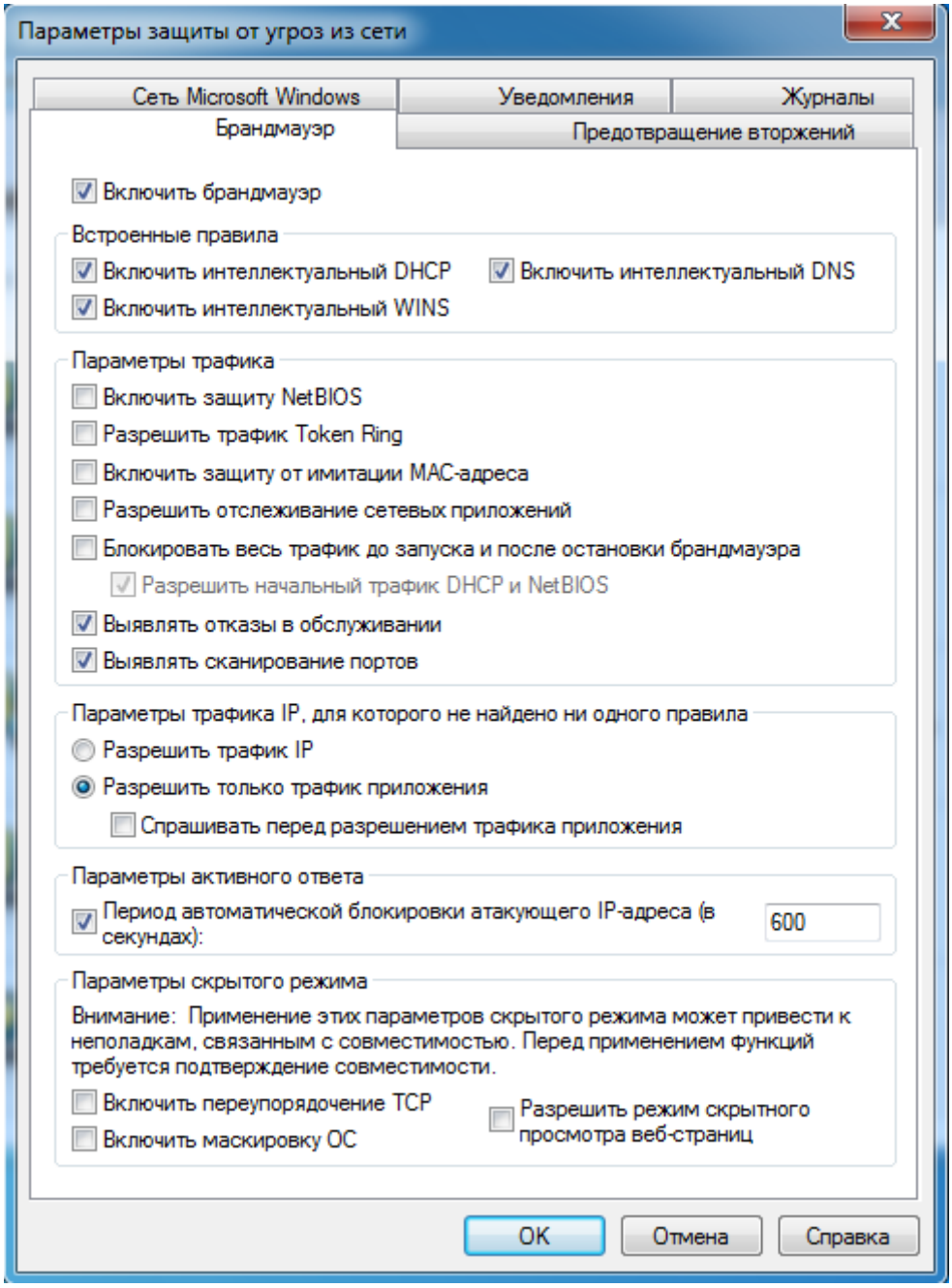

Рис.3.8. Налаштування роботи брандмауера SymantecEndpointProtection

На вкладці «Запобігання вторгнень» можна включити або відключити захист мережі і захист браузера від вторгнень. На вкладці «Сеть Microsoft Windows» можна вказати конкретний адаптер, або вибрати всі наявні адаптери для контролю трафіку, а також заблокувати доступ до деяких системних або користувача мережевих ресурсів ззовні. На вкладці «Повідомлення» можна

включити відображення повідомлень, а також звукового оповіщення. Нарешті, вкладка «Журнали» визначає для кожного типу журналів його максимальний розмір і час зберігання записів в ньому.

Параметри винятків реалізовані у вигляді єдиного вікна, в якому можна вказати відомі загрози на ім'я детектування, файлів, папок, розширень, веб-доменів, а також виключення об'єктів з перевірки технологією SONAR. Також можна виключити програми з перевірки цілком.

Остання група налаштувань об'єднана заголовком «Управління клієнтами», і ці настройки розбиті на 4 вкладки. Вкладка «Загальні» присвячена параметрам відображення інтерфейсу клієнта Symantec Endpoint Protection, параметрам проксі-сервера, параметрам перезавантаження для різних ситуацій, а також управління додатками і пристроями. Вкладка «Захист від змін», по суті, присвячена налаштувань роботи самозахисту антивіруса. Вкладка LiveUpdate містить настройки, що визначають параметри автоматичного оновлення продукту. Заключна вкладка «Відправка» містить прапорці, що відповідають за необхідність відправки того чи іншого типу інформації в хмару Symantec для допомоги протидії зловмисникам і допомоги в розробці наступних версій SEP.

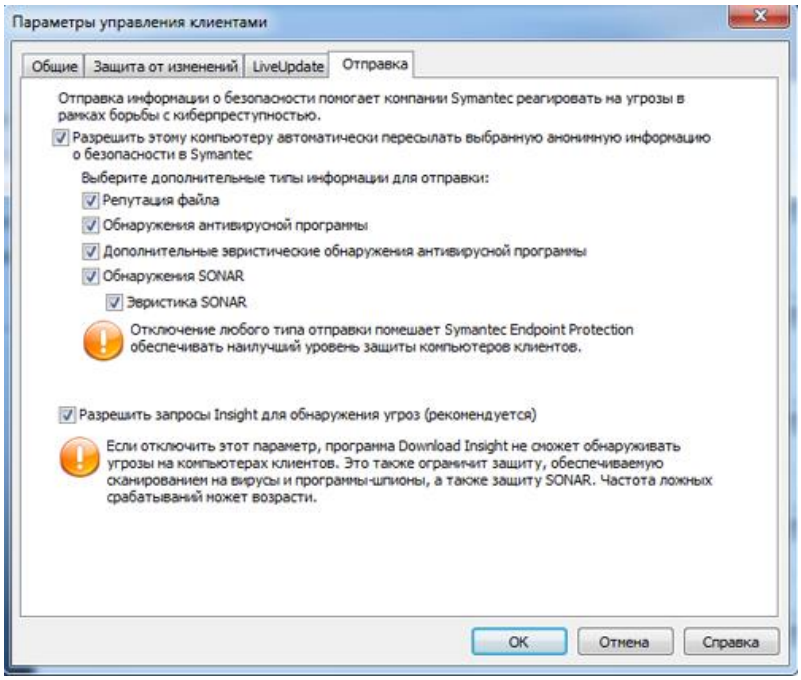

Рис.3.9. Параметри управління клієнтами в SymantecEndpointProtection

Пункт меню «Карантин» в головному вікні інтерфейсу Symantec Endpoint Protection для Windows має досить стандартний інтерфейс. Файли, що знаходяться в ньому, можна відновити, видалити, повторно просканувати і експортувати. Також в карантин можна додати будь-який підозрілий файл, або відправити його на аналіз в компанію Symantec. Параметри очищення розбиті на три вкладки: «Об'єкти в карантині», «Копії заражених файлів» і «Виправлені файли». Для кожного з типів об'єктів можна налаштувати час їх зберігання в карантині, а також максимальний розмір сховища.

Пункт меню «Показати журнали» головного вікна інтерфейсу клієнта Symantec Endpoint Protection для Windows містить кнопки, за допомогою яких можна відобразити журнали, що відповідають кожному компоненту антивірусного захисту. В даних журналах можна знайти детальну інформацію про роботу кожного компонента Symantec Endpoint Protection для Windows і, в разі виникнення проблем в роботі антивірусного клієнта, досить швидко їх локалізувати.

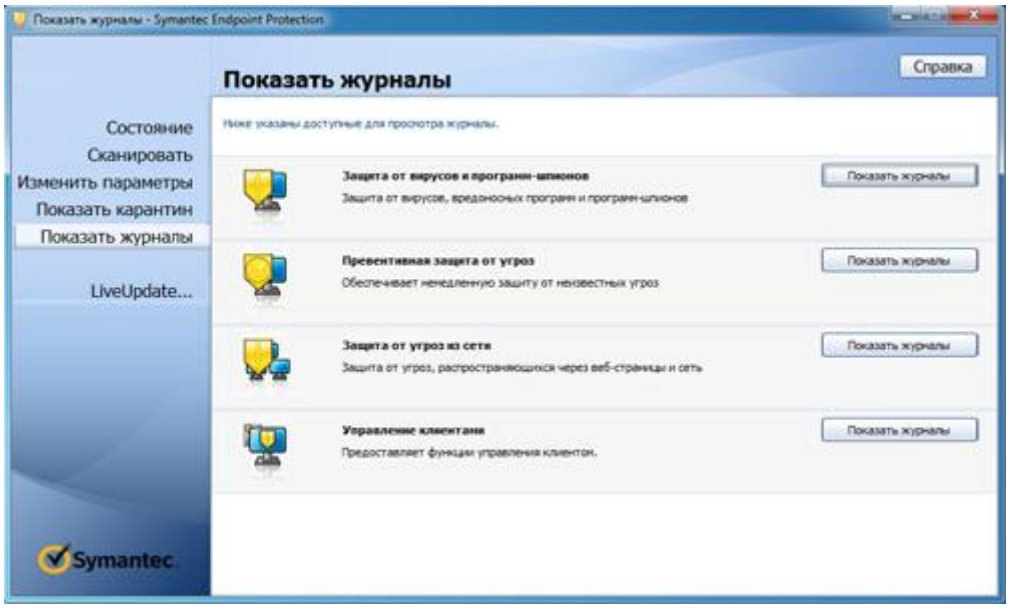

Рис.3.10. Список компонентів з можливістю відображення журналів їх роботи в SymantecEndpointProtection

У головному вікні клієнта Symantec Endpoint Protection для Windows також доступна кнопка Довідка, клацнувши по якій можна вибрати, крім іншої

інформації, пункт «Пошук та усунення несправностей». При цьому відображається вікно з докладною інформацією про налаштування системи і антивірусного клієнта. Ця інформація може бути дуже корисною, наприклад, при зверненні в технічну підтримку.

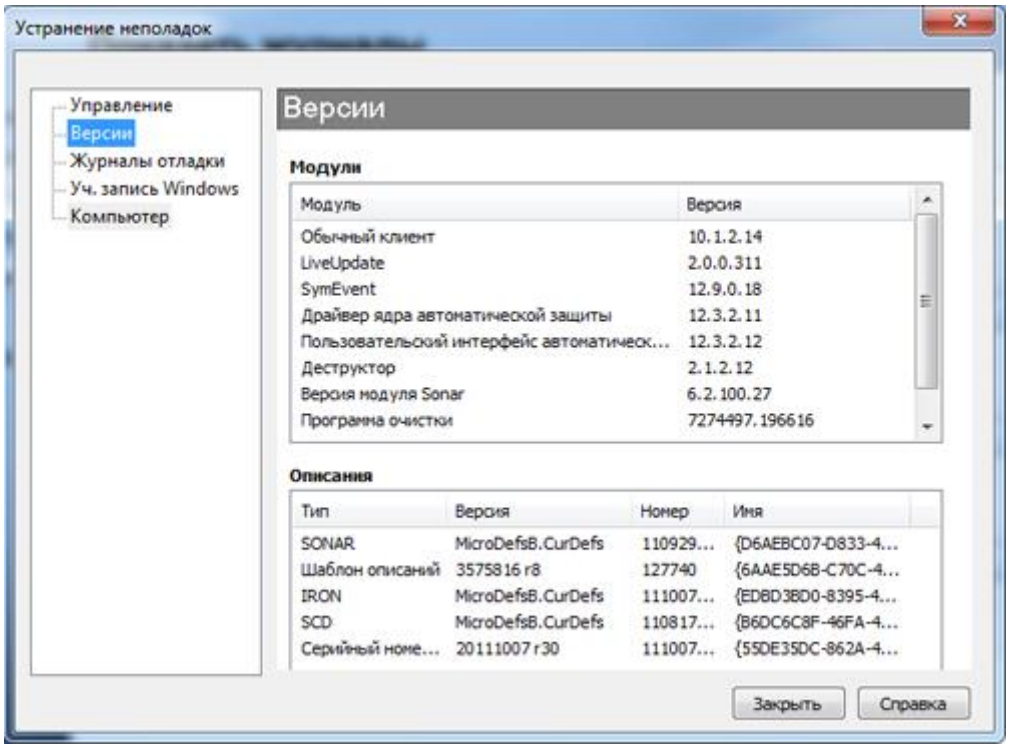

Рис.3.11. Вікно «Пошук та усунення несправностей» в клієнті SymantecEndpointProtection

ВИСНОВКИ

В роботі проведено дослідження технологій захисту кінцевих пристроїв за допомогою продуктів Endpoint Protection Platform. Визначено Їх сучасні завдання та вимоги до них.

Проаналізовано ринок Endpoint Protection Platform, коротко розглянуто його найсильніших представників, серед яких більш детально розглянуто компанію Symantec. На основі аналізу ринку та стану конкуренції на ньому виявлено тенденції його подальшого розвитку.

Встановлено основні функції та принципи роботи програмного комплексу Symantec Endpoint Protection. Визначено технології, що використовуються у даному продукті такі як Insight, Bloodhound і SONAR, що виводить захист на якісно новий рівень. При цьому кожен з компонентів захисту можна налаштовувати досить точно для знаходження найкращого балансу між якістю захисту, необхідними апаратними ресурсами, а також кількістю помилкових спрацьовувань.

Також антивірусні складові клієнта Symantec Endpoint Protection оснащені компонентами, що дозволяють контролювати запуск користувачем додатків і підключення змінні пристроїв. Робота цього клієнта оптимізована для використання у віртуальних середовищах. Також до складу цього продукту входить функція запобігання експлуатації уразливості браузерів. Адже браузери сьогодні беруть участь в переважній більшості схем зараження системи. І всі ці технології разом перетворюють Symantec Endpoint Protection в надійний злагоджений механізм захисту від сучасних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Блог Trend Micro про захист кінцевих точок: https://habr.com/ru/company/trendmicro/blog/450136
2. SOVIT security – комплексний захист кінцевих точок: http://sovit-security.ru/interesno/endpoint_security/
3. Олексій Матвєєв – Ринок систем захисту канцевих точок: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform#part2
4. Лідери ринку Endpoint Protection Platform: https://www.tadviser.ru/index.php/
5. Огляд Symantec Endpoint Protection: https://heritage-offshore.com/net-admin/obzor-symantec-endpoint-protection/
6. Корпоративний комплексний антивірус Symantec Endpoint Protection: https://hapers.ru/korporativnyj-kompleksnyj-antivirus-symantec-endpoint-protection/
7. Валерій Лєдовской – Компоненти клієнта Symantec Endpoint Protection: https://www.anti-malware.ru/reviews/Symantec_Endpoint_Protection_12_1#part7
8. Charles J. Brooks, Philip R. Craig, Donald ShortCybersecurity Essentials. – SYBEX. 2018.
9. Chris Moschovitis Cybersecurity Program Development for Business: The Essential Planning Guide. – WILEY. 2018.
10. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam Enterprise Cybersecurity Study Guide. – 2018.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)