Антивірус нового покоління і його роль у кіберзахисті

NGAV — це дещо більше, ніж стара ідея на новий лад.

Для захисту кінцевих точок існують рішення EPP і EDR, а як щодо старого доброго антивіруса? Він еволюціонував, перетворившись на антивірус нового покоління (NGAV). Використовуючи штучний інтелект і машинне навчання, ці рішення виявляють раніше не відомі зловмисні програми, а також зупиняють атаки, що здійснюються без зловмисного ПЗ. NGAV працює в хмарі з усіма перевагами цієї моделі, як-от швидке розгортання і відсутність витрат на підтримку.

«МтБ» спробував розібратися, яке місце займають антивіруси нового покоління в архітектурі кібербезпеки, що пропонують виробники і чи потрібен взагалі такий клас рішень.

NGAV vs AV

Перші антивірусні програми з'явились у 1980-х невдовзі після перших власне вірусів. Згодом постали такі відомі бренди, як McAfee, NOD, Avira, Avast, Norton та інші. У 1990-х, коли відбувалось розростання Інтернету, ним почали поширюватися й віруси, що стимулювало й розвиток захисних програм. Тоді антивіруси використовували сигнатурний аналіз, порівнюючи файли з базою даних відомих вірусів. У нульових виробники зосереджувались на додаткових функціях та розширені охоплення продукту (з'явились версії для мобільних пристроїв Apple).

Між тим відбувались дві речі. По-перше, кількість зразків зловмисного ПЗ невпинно зростала з року в рік. Відповідно збільшувались бази сигнатур, а ще ж були поліморфні віруси, здатні змінювати власний код. Виробники почали вивантажувати антивірусні БД у хмари, але на той час швидкість з'єднань, а також обчислювальна потужність комп'ютерів робили процес перевірки нешвидким. Окрім того, ставали «важчими» самі антивірусні програми, забираючи багато ресурсів ПК. Як писав у 2016 році Девід Поттер, старший менеджер з рішень кібербезпеки компанії Arrow: «... у багатьох випадках ліки гірші за хворобу: ваш антивірус такий великий, що ваш комп'ютер ніц не робить, тільки безперервно сканує файли на віруси».

Табл. Порівняння EDR, EPP і NGAV (джерело: Sangfor)

Аспект	EDR	EPP	NGAV
Головне призначення	Виявлення загроз і реагування на них	Відвернення, виявлення і реагування + управління кінцевими точками	Превентивний захист від складного зловмисного ПЗ
Основна функція	Виявлення і розслідування підозрілої активності	Захист кінцевих точок від загроз і атак Виявлення підозрілих подій	Превентивний захист від атак з використанням складного зловмисного ПЗ і вразливостей нульового дня
Ключові можливості	Безперервний моніторинг Полювання на кіберзагрози Реагування на інциденти Негайне відновлення	Антивірус + NGAV EDR Функції управління	Машинне навчання Поведінковий аналіз Відвернення експлойтів Хмарна кіберрозвідка
Підхід до моніторингу	Поведінковий аналіз у реальному часі	Сигнатурне й евристичне сканування Захист у реальному часі, який включає поведінковий моніторинг з використанням ШІ	Аналіз поведінки і патернів за допомогою МН/ШІ
Механізм реагування	Генерація сповіщень і кероване реагування	Ізоляція і нейтралізація загроз	Проактивне запобігання загрозам та їх ізоляція
Ідеальна управлінська команда	Аналітики безпеки та команди реагування на інциденти	Адміністратори кібербезпеки Аналітики кібербезпеки IT-адміністратори	Команди IT-безпеки з прицілом на складні загрози
Протистояння загрозам	Має справу зі складними і стійкими загрозами	Усеохопний захисний щит, який закриває усі вектори загроз — і відомі, і невідомі, і комплексні	Бореться з комплексними загрозами, що еволюціонують
Додаткові функції	Ізоляція кінцевих точок Інтеграція з кіберрозвідкою Інтеграція з SIEM	Контроль USB Управління ресурсами Віддалена допомога Виявлення файлових і безфайлових загроз Захист від кіберздирництва Єдиний захист кінцевих точок	Виявлення безфайлових зловмисних програм Хмарне розгортання

По-друге, ландшафт загроз також невпинно змінювався. Здирницьке ПЗ (Ransomware), безфайлові загрози, атаки з використанням вразливостей нульового дня, а також складні стійкі атаки типу APT, — усе це ставило питання про зміну концепції антивіруса, щоб він міг засікати усі види загроз, так само як і досі не відомі.

Антивірус нового покоління використовує предиктивну аналітику на основі штучного інтелекту і машинного навчання. Він здатен виявляти і зупиняти атаки як з використанням зловмисного ПЗ, так і безфайлові, боротися як з добре відомими, так і з невідомими загрозами, за допомогою поведінкового аналізу виявляти і зупиняти атаки на базі вразливостей нульового дня, збирати докладну телеметрію для подальшого розслідування. А позаяк NGAV працює з хмари, його можна розгорнути і запустити за кілька днів замість кількох діб, він споживає мало ресурсів кінцевого пристрою, не потребує додаткового апаратного чи програмного забезпечення і гарно масштабується під потреби бізнесу.

NGAV vs EPP vs EDR

Захист пристроїв давно не обмежується антивірусом, адже існують інші класи рішень: EDR (Endpoint Detection & Response) і EPP (Endpoint Protection Platform). Де серед них місце для антивіруса?

Як стисло пояснює компанія ReasonLabs, фактично організаціям потрібно обирати між EPP і NGAV залежно від їхніх конкретних потреб і загроз. Якщо коротко, то EPP виконує широкий спектр функцій захисту, тоді як NGAV бере на себе виявлення складних загроз і реагування на них. При цьому антивірус використовує поведінковий аналіз і штучний інтелект задля більш досконалого і адаптивного виявлення загроз, тоді як EPP може послуговуватись більш традиційними методами на основі сигнатурного аналізу. По-третє, NGAV часто працює з хмари, тоді як для рішень EPP використовується більш традиційна модель розгортання.

Що стосується EDR, то його функцією є виявлення підозрілої активності у реальному часі і запобігання атакам. EDR збирає дані з кінцевих точок, шукає патерни, які вимагають розслідування і реагування, видає відповідні сповіщення з усім необхідним контекстом і забезпечує ізоляцію і нейтралізацію. Іншими словами, він працює з атаками, які вже здійснюються, і не дає їм поширюватися. Як у цьому зв'язку зауважує компанія CrowdStrike, NGAV є компонентом превентивного захисту, мета якого — не дати загрозам потрапити в мережу. Він є першою лінією оборони, тоді як EDR — це рятувальна сітка, яка ловить загрози, що вже проникли всередину.

А ось таке порівняння функцій і можливостей всіх трьох класів рішень зробила компанія Sangfor (**таблиця**).

При цьому, хоча атаки справді починаються на кінцевих точках, для повноцінного захисту все одно потрібно мати й інші інструменти.

Ключові вимоги до NGAV

В Інтернеті можна знайти чимало описів того, чим є NGAV і що він повинен уміти. Ось, наприклад, які поради щодо вибору продукту формулює компанія Security Tools.

По-перше, NGAV повинен детектувати широкий спектр знайомих і незнайомих загроз, зокрема складне зловмисне ПЗ, атаки через вразливості нульового дня і таргетовані атаки, і захищати від отого всього. При цьому він повинен мати потужні механізми детектування, зокрема поведінковий аналіз, машинне навчання і інтегровану кіберрозвідку.

По-друге, NGAV повинен працювати на всіх типах кінцевих точок, які є в організації, від ПК і серверів до мобільних пристроїв і IoT. Також при замовленні організаціям варто врахувати повноту захисту для всіх операційних систем. Окрім того, рішення має забезпечувати заощадження часу і роботи завдяки простоті і швидкості інсталяції та оновлень, а також масштабування, щоб задовольняти потреби бізнесу при розширенні, і безпроблемне підключення нових пристроїв.

По-третє, потрібно забезпечити інтеграцію NGAV з наявними в компанії інструментами кібербезпеки, такими як SIEM і EDR. Рішення повинне забезпечувати баланс між потужним захистом і мінімальним використанням обчислювальних ресурсів, і ефективно працювати за відсутності інтернет-з'єднання.

Нарешті, на рішення повинна бути гнучка модель ціноутворення, яка враховує бюджетні обмеження і потреби бізнесу, а також воно має забезпечувати прийнятну рентабельність інвестицій (ROI), виходячи з характеристик його роботи і довготермінової цінності.

При цьому, зазначає Security Tools, використання рішень NGAV пов'язане і з певними викликами. По-перше, вони все ж таки споживають деяку кількість системних ресурсів, що потенційно може спричиняти сповільнення роботи, якщо ці ресурси обмежені, або викликати потребу в перезавантаженні для активації нових можливостей захисту.

По-друге, впровадження рішень NGAV все ж може потребувати початкового конфігурування та налаштування під потреби організації, що займе деякий час.

Приклади

В Інтернеті не так багато об'єктивних рейтингів NGAV, що базуються на замірах їхніх характеристик. Одне таке тестування проводив у вересні-жовтні 2024 року німецький інститут AV-TEST: перевіряв роботу 17 продуктів для захисту кінцевих точок, використовуючи при цьому найновішу доступну в продажу версію продукту з налаштуваннями, вказаними виробником. При цьому було дозволено оновлення продуктів і звертання до відповідних хмарних сервісів. У ході випробувань використовувались реалістичні сценарії і актуальні загрози, продукти ж мали продемонструвати роботу усіх своїх складових і рівнів захисту.

Антивіруси перевірялись за трьома критеріями: захист (здатність протидіяти зловмисному ПЗ та іншим кіберзагрозам); продуктивність (швидкість та ефективність роботи антивіруса для різних операційних систем); зручність (статистика хибних тривог і загалом користувацький досвід). За результатами досліджень 9 продуктів від 7 компаній отримали найвищий рейтинг, серед них — BitDefender, Avast, ESET і Microsoft.

А ось кілька прикладів рішень, які позиціонуються на ринку саме як NGAV. Здебільшого вони входять до складу більш широких платформ кібербезпеки, які також включають функції EDR, кіберрозвідки, захисту облікових даних тощо.

CrowdStrike Falcon Prevent: входить до складу платформи Falcon, в основі рішення лежить невеликий агент, який встановлюється за кілька хвилин, працює

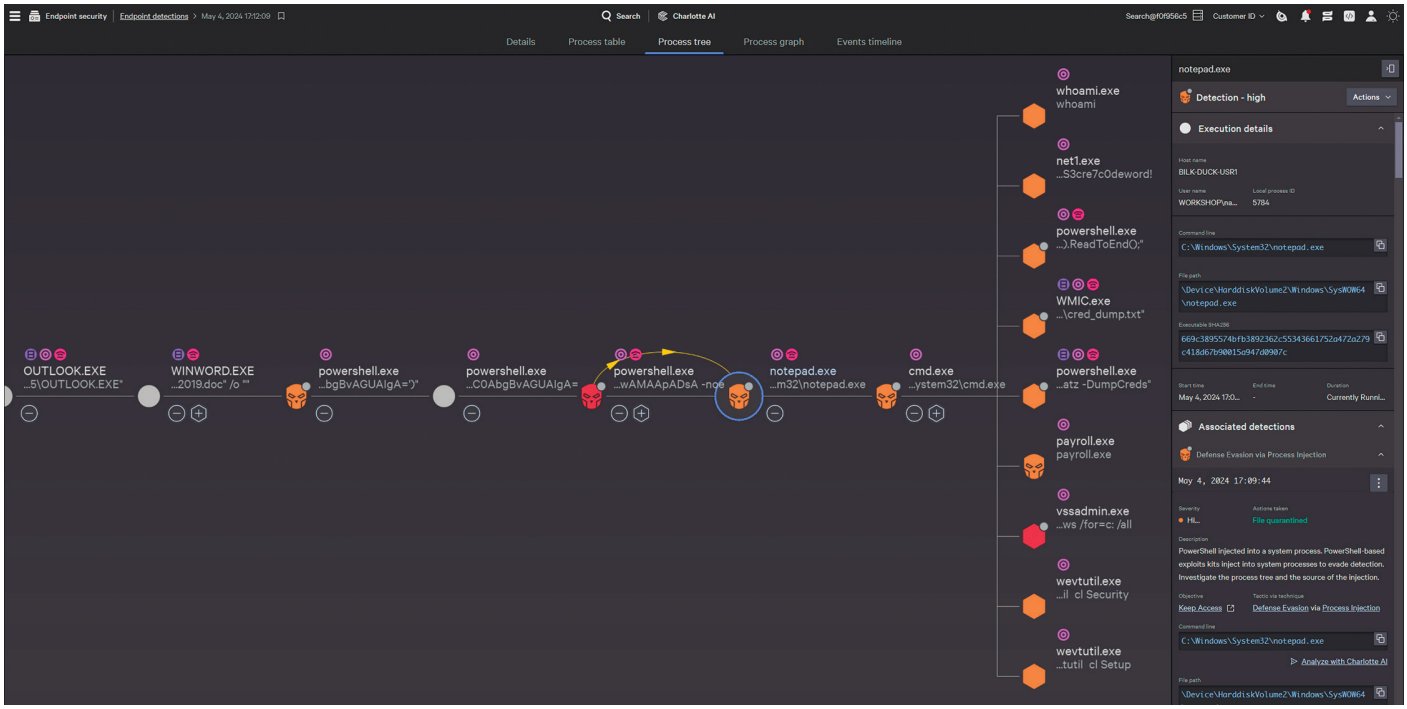

Рис. 1. Візуалізація атаки в CrowdStrike Falcon Prevent

без постійних оновлень сигнатур і не створює значного навантаження на процесор, забезпечує автоматизоване реагування на індикатори атаки (IOA) і знищує артефакти, які можуть призвести до повторного зараження. Інтеграція з сервісом кіберрозвідки CrowdStrike Falcon Adrersary Intelligence забезпечує розуміння загроз у корпоративному середовищі, дозволяє пріоритизувати заходи реагування, негайно давати раду інцидентам на основі глибокого аналізу загроз. Також Falcon Prevent надає повний контекст і історію кожного сповіщення і відображає атаку у вигляді дерева процесів, зберігаючи ці дані протягом 90 днів (**рис. 1**).

SentinelOne Singularity Core. Теж використовує агент під назвою Storyline, який в реальному часі вибудовує контекст атаки з пропонованими діями щодо реагування. Цей агент на основі ШІ замінює сигнатурний аналіз і може працювати автономно без звертання до хмари. Також за допомогою поведінкового аналізу агент може виявляти і зупиняти безфайлові атаки в реальному часі. Фірмова функція One-Click remediation & rollback відновлює дані до стану, який передував несанкціонованим змінам. Для розслідування інцидентів забезпечуються докладні дашборди з анотаціями, хронологією та іншими даними (**рис. 2**).

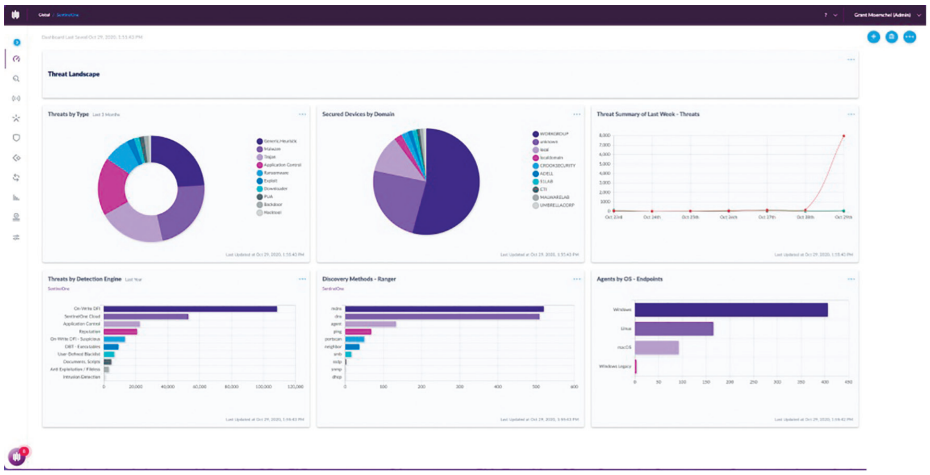

Рис. 2. Дашборд SentinelOne Singularity Core з даними про атаку

VMware Carbon Black Cloud Endpoint Standard. Особливість цього рішення — поєднання в одному агенті функцій NGAV і EDR. Рішення може працювати в трьох режимах: моніторинг (відстежує активність на пристроях і виводить дані про події на дашборд, який потім можна завантажити для звітності (**рис. 3**): стандартний — блокує відоме зловмисне ПЗ і підозрілі програми, а також ризиковані операції на кшталт сканування пам'яті і ін'єкції коду; просунутий — забороняє операціям доступ до системних ресурсів і зупиняє ризиковані дії, які загалом можуть бути фальшивою тривогою.

Endpoint Standart використовує багаторівневий захист, а саме: хмарний репутаційний сервіс (сигнатури, відкладений запуск зі скануванням алгоритмами машинного навчання); AMSI (автоматичний аналіз і блокування шкідливих скриптів); налаштування правил протидії для обмеження чи заборони невідомим/необлікованим застосункам виконувати небажані дії; «файли-канарки» — розміщення приманок у файловій системі для запобігання шифруванню.

HP Sure Sense. Це елемент платформи захисту кінцевих точок HP Wolf Security, який базується на технології глибокого машинного навчання. Автономний агент Sure Sense, який може працювати онлайн і офлайн, займає 30 Мбт пам'яті і в фоновому режимі забирає 1% ресурсів процесора. Оновлення агента відбувається щотримісяці. Як стверджує виробник, рішення забезпечує відвернення загроз протягом 20 мс, розслідування — 50 мс, відновлення і стримування — менш ніж за хвилину. Згідно з описом Sure Sense також може виявляти і зупиняти атаки типу APT 3 точністю понад 99%. Також рішення зупиняє здирницьке ПЗ ще до його запуску і відсилає на карантин.

Fortinet Unified FortiClient. Цей програмний агент, як видно з назви, забезпечує багато чого: захищений доступ за допомогою VPN або ZTNA, URL-фільтрацію і функції брокера доступу до хмарних сервісів (CASB). Додатковий рівень захисту забезпечують функції NGAV, а також карантину кінцевих точок, мережевого екрана прикладного рівня, хмарної пісочниці, контролю USB і протидії програмам-здирникам.

Звичайно, рішень NGAV набагато більше, але часто їх важко виріznити серед функціональності інтегрованих продуктів безпеки. Зате можна з певністю сказати, що поховання антивіруса, про яке говорили у середині минулого десятиліття, не відбулося.

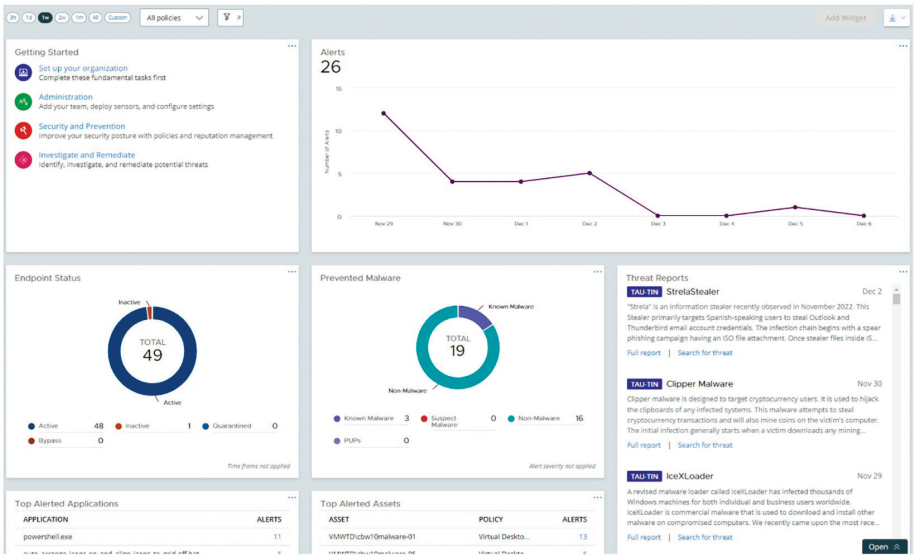

Рис. 3. Дашборд Carbon Black Cloud Endpoint Standard

Василь ТКАЧЕНКО, МтБ