Кіберзахист починається з кінцевих точок

Хакери потрапляють у мережу так чи інакше через пристрої користувачів. Але старого доброго антивірусу вже замало, щоб їх зупинити.

Платформа захисту кінцевих точок (EPP) — це в певному сенсі еволюція антивірусу з метою захисту від нових загроз, таких як безфайлові атаки і вразливості нульового дня. Окрім сигнатурного аналізу, EPP використовує поведінковий, а також чорні і білі списки, динамічний аналіз коду в пісочниці і статичний за допомогою штучного інтелекту, моніторинг пам'яті та інші функції. Споріднений клас рішень з виявлення та знешкодження загроз на кінцевих точках (EDR) виходить з того, що злам вже стався, і забезпечує не лише пошук ознак атаки, а й реагування, аналіз і розслідування. Ці рішення розглядають як окремі, або ж EDR і його розширена версія XDR вважаються частиною EPP (наприклад, за класифікацією Gartner).

«МтБ» розповідає, як працюють системи захисту кінцевих точок, що пропонують виробники і як технології розвиватимуться надалі.

EPP, EDR і XDR як король всього

За даними Verizon, які часто цитують, 70% інцидентів з витоком даних стаються через кінцеві точки. Як зазначає у своєму аналізі компанія Netwrix, перехід до гібридного режиму роботи ставить перед відділами кібербезпеки компаній нетривіальні завдання. По-перше, кількість кінцевих точок, які мають доступ до даних, невпинно збільшується, і всі вони різні, адже мають відмінні операційні системи, застосунки, стан підключення тощо. По-друге, користувачі вже не залишаються в корпоративній мережі, а воліють підключатися з будь-якого місця. І, по-третє, застосунки для колективної роботи значно посилили рух даних між користувачами і компаніями.

Захистом кінцевих точок і даних, які там є, займаються, як не дивно, рішення для захисту кінцевих точок. Незважаючи на присутність у їхній назві слова ***endpoint***, вони мають різний набір функцій.

Можна знайти різні визначення EPP, проте в чистому вигляді ці рішення покликані захищати кінцеві точки (комп'ютери, мобільні пристрої, принтери і т.д., загалом будь-яке підключене до мережі обладнання) від загроз. Для цього вони використовують сигнатурний і поведінковий аналіз, перевіряють файли в пісочниці і блокують небезпечні IP-адреси. EDR захищають від складних сталих загроз (APT) і зловмисних програм, створених для обходу традиційних інструментів безпеки, вони аналізують патерни даних, автоматично блокують загрози, а також записують зловмисну поведінку для подальшого розслідування.

Термін XDR (eXtended Detection&Response) вперше запропонувала компанія Palo Alto Networks у 2018 році, а у 2020-му його визнав Gartner і визначив як «єдину платформу виявлення інцидентів та реагування на них, яка автоматично збирає та зіставляє дані з існуючих компонентів системи безпеки» (станом на 2023-й визначення дещо розширилось). Вважається, що XDR є гарним варіантом для підприємств СМБ, які не мають коштів на створення комплексної системи захисту з рішеннями на кшталт SIEM і SOAR, але при цьому все одно потребують захисту, зокрема для своїх хмарних ресурсів і мобільних працівників.

Як пише Forbes у статті *Where Does XDR Go From Here?* («Куди далі попрямує XDR?», вересень 2023 року), концепція з'явилась як розширення зрілих рішень — для мереж (NDR) і для кінцевих точок (EDR). Оскільки історично в організаціях мережі і пристрої захищались окремо і по-різному, постала потреба об'єднати технології і нормалізувати дані, щоб персонал, який відповідає за безпеку, міг їх розуміти і вживати заходів. («Коротше кажучи, XDR є дітищем індустрії, яка славиться своїм умінням розробляти рішення для проблем, що їх допомогли створити старі рішення», — уїдливо зазначає автор).

Що таке, врешті, XDR і як він співвідноситься з EPP, теж предмет суперечок, проте загалом це певна уніфікована платформа безпеки, яка поєднує функції різних продуктів і замінює більш традиційні рішення, такі як EDR, SIEM і аналізатори мережевого трафіку (NTA). Робота XDR відбувається в три етапи (**рис.**) На першому система збирає дані з різних джерел, зокрема власне кінцевих пристроїв, мережі та хмари, аналізує їх і створює контекст для сповіщень, які генеруються. На другому етапі XDR виокремлює загрози, які є критичними і вимагають втручання. На третьому XDR самостійно нейтралізує ці загрози і оновлює політики безпеки, щоб подібні інциденти не повторювалися. Тобто фактично XDR перебирає на себе роль SIEM.

Рис. Схема роботи XDR (джерело: Spice Networks)

«Хвиля» Forrester

Компанія Forrester у своєму звіті *The Forrester Wave: Extended Detection And Response Platforms, Q2 2024* зазначає, що у 2021 році вендори пропонували мішанку функцій з метою замінити SIEM як основну технологію SOC. Зараз же багато з них досягли такого рівня інтеграції і функціональності, що замовники вже потроху беруться до заміни SIEM, хоча XDR все ще не можуть конкурувати за деякі ніші застосування SIEM. З іншого боку, нещодавні потрясіння на ринку SIEM (уточнимо: купівля Cisco Splunk, злиття Exabeam і LogRhythm, купівля Palo Alto QRadar у IBM) створюють для виробників XDR шанс продемонструвати замовникам, як може виглядати новий підхід.

Forrester оцінює продукти за трьома групами критеріїв: поточна пропозиція (зважені технічні параметри і можливості продукту), стратегія (візія, інновації, дорожня карта, партнерська екосистема, гнучкість та прозорість ціноутворення, спільнота) і ринкова присутність (дохід, кількість замовників). «Хвиля» являє собою фрагменти концентричних сегментів кілець у куті квадрата, де вертикальна вісь відповідає силі поточної пропозиції, горизонтальна — стратегії, а компанії відображаються у вигляді кругів, розмір яких відповідає ринковій присутності. Внутрішній сегмент посідають лідери ринку, за якими розташовуються «сильні гравці» (Strong Performers), ближні і дальні претенденти (Contenders і Challengers).

За цим рейтингом до кола лідерів віднесено Microsoft, Palo Alto і CrowdStrike, причому перша має взагалі найбільшу ринкову присутність серед оцінюваних компаній. За ними в категорії сильних гравців знаходяться Trend Micro, Bitdefender і SentinelOne.

Зокрема, за оцінкою дослідників Forrester, Microsoft має найбільш повну XDR-пропозицію на ринку, а також найбільш повну телеметрію від кінцевих точок, можливість реагувати на сповіщення за допомогою інтегрованих інструментів (Microsoft Defender), потужну пісочницю та інше. У Palo Alto дослідники відзначають унікальний «розчинний» агент, який, який можна автоматично розгорнути для опитування некерованого хоста у випадку аномалії, широкий набір власних і сторонніх інструментів виявлення загроз, а також чат для розслідувань. А про CrowdStrike сказано, що компанія виділяє на дослідження і розробки більший за середній відсоток від прибутку, фокусуючись на використанні ШІ та вдосконаленні технологій кореляції з довготерміновим прицілом на ринок SIEM.

«Магічний квадрант» Gartner

З іншого боку, Gartner відносить XDR до розширеної функціональності EPP (EDR — до основної). Gartner визначає EPP як програмне забезпечення, призначене для захисту керованих кінцевих точок, зокрема персональних комп'ютерів, ноутбуків і мобільних пристроїв, проти відомих і невідомих атак. Окрім того, воно має надавати фахівцям з кібербезпеки можливості для розслідування інцидентів, які обходять засоби виявлення, і усунення їх наслідків. EPP-продукти постачаються як програмні агенти, що встановлюються на кінцеві точки і підключаються до централізованих інтерфейсів аналітики і управління. EPP повинна забезпечувати захист від відомих і невідомих загроз і працювати як елемент стратегії ешелонованої оборони задля скорочення поверхні атаки і мінімізації збитків.

Стандартними функціями EPP, за визначенням Gartner, є захист від загроз, зокрема файлових і безфайлових; вміння виявляти і блокувати загрози з використанням поведінкового аналізу; вміння фіксувати і розслідувати інциденти та допомагати з усуненням їх наслідків, якщо загрози уникають виявлення; керування сповіщеннями вбудованих засобів операційної системи, таких як фаєрвол і контроль підключених пристроїв; функції EDR. До додаткових можливостей належать: вміння готувати звіти щодо ризиків, пов'язаних з кінцевими пристроями; пошук вразливостей на пристроях і управління встановленням патчів; XDR з модулями захисту облікових записів, електронної пошти і серверів; підтримка вендорських сервісів на кшталт пошуку загроз, керованого виявлення і знешкодження загроз (MDR) і цифрового розслідування та реагування на інциденти (DFIR); подовження терміну підтримки застарілих і маловживаних операційних систем.

Gartner зазначає, що EPP є найпоширенішим шаром захисту від зловмисних програм і основою базової безпекової гігієни. При цьому 90% організацій використовують хмарні рішення EPP. Близько 57% використовують функції EDR — на 15% більше, ніж було у 2022-му. Дедалі більша складність рішень і брак кваліфікованого персоналу призводять до зростання популярності керованих сервісів, які забезпечують моніторинг і розбір інцидентів (на них вже підписані близько 17% організацій). Окрім того, Gartner відзначає, що ринок більше не обмежується чистими виробниками EDR і EPP, бо покупці намагаються обходитись меншою кількістю вендорів і обирають тих, які пропонують ширші функції. Зокрема захист пошти і виявлення та усунення загроз, пов'язаних з обліковими записами (ITDR), оскільки витоки даних зазвичай стаються в результаті фішингу і крадіжки акаунтів.

Деякі вендори позиціонують свої продукти як зрілі і розраховані на повністю укомплектовані відділи кібербезпеки, інші пропонують рішення, які є простішими у використанні і надають контекстуальні підказки. Багато виробників анонсували або вже випробовують функції розслідування на базі штучного інтелекту.

Gartner нарахував у своєму «квадранті лідерів» за 2023 рік 6 компаній, зокрема «лідерами серед лідерів» можна назвати CrowdStrike і Microsoft, далі SentinelOne, Trend Micro, Palo Alto Networks і Sophos. Зокрема серед сильних сторін CrowdStrike дослідники відзначають інноваційність, функції хмарного захисту, управління поверхнею атаки та ITDR, зрілу функціональність EDR, широкий спектр телеметрії, легкий агент і керовані сервіси (оцінювали ще до липневого інциденту). У Microsoft вони відзначили універсальність пакету захисту робочих місць та інтеграцію з власною Sentinel SIEM, широкі можливості конфігурування і широкий спектр телеметрії, доступний за замовчанням.

Palo Alto інтегрує функції захисту робочого простору в Cortex XDR, також відзначено високий рівень налаштовуваності, взаємосумісності і автоматизації. Окрім того, вендор підтримує більше хмарних точок присутності за середній рівень і локалізацію багатьма мовами. Сильними сторонами Trend Micro є інтеграція управління поверхнею атаки, управління конфігурацією безпеки і функцій XDR в платформі Vision One, яка забезпечує проактивне скорочення ризиків (тут аналітики також виділяють недавнє включення ITDR). Іншими особливістями є підтримка застарілих ОС і загалом нижча вартість порівняно з іншими лідерами.

Еволюція захисту

Досвід підказує, що технічні рішення, які мають у своїй назві щось на кшталт «Extended», «Evolved» або «Next-Generation», з часом усе одно застарівають і не те щоб йдуть з ринку, але можуть виявитися недостатніми. Це теж не гарантований фінал — врешті, мережеві екрани наступного покоління вже ховали, а вони досі живі. XDR з'явився лише відносно недавно, і найближчим часом це йому вочевидь не загрожує. Продовжує розвиватися і EPP. Одним з напрямків є, як і скрізь, залучення штучного інтелекту, в даному разі для кореляції даних з різних джерел, виявлення патернів і детектування аномалій.

Наприклад, Trellix позиціонує своє рішення Trellix Endpoint Security як платформу захисту наступного покоління, яка базується на штучному інтелекті, машинному навчанні (МН) і тісній інтеграції функцій захисту мереж і кінцевих точок. Платформа забезпечує антивірусний захист, функції мережевого екрана і захисту з'єднань, а також використовує МН для виявлення вразливостей нульового дня, підозрілих програм і дій. Більш того, на основі МН система сама вирішує, які дані і коли збирати, як це вплине на користувача (швидкість, затримка) і як часто модель потрібно калібрувати через зміну процесів і політик.

Рішення SentinelOne його розробник, компанія Bridgenet, так само називає EPP наступного покоління з EDR. (Forrester зазначає, що SentinelOne «все ще еволюціонує» до XDR). За твердженням Bridgenet, платформа використовує статичний і поведінковий аналіз за допомогою ШІ, а також дані глобальної кіберрозвідки. Можливість автономного прийняття рішень забезпечує миттєву реакцію. Окрім того, SentinelOne записує всю хронологію атаки для подальшого розслідування. А також дозволяє відкотити систему до стану перед зараженням і так відновити файли, зашифровані кіберздирниками.

А куди рухається XDR? Аналітик Гілад Давид Мааян на сайті HackerNoon окреслює наступні кроки. По-перше, це дедалі більше залучення цього інструмента компаніями сегмента СМБ, які зазвичай не поспішають запроваджувати передові системи кіберзахисту через брак грошей або необізнаність. XDR, корелюючи дані з різних джерел, створює цілісну картину і дає змогу швидко виявляти загрози і реагувати. Понад те, XDR замінює собою розрізнені рішення, що підвищує операційну ефективність.

По-друге, ринок потроху посувається до моделі XDR-as-a-Service, яка не лише дозволяє заощадити і забезпечує швидку адаптацію до потреб компанії і зміни загроз, але й дає змогу скористатися досвідом фахівців компанії-постачальника.

Передбачається, що XDR будуть забезпечувати захист не лише традиційних кінцевих точок, але й пристроїв IoT. Це важливо, бо IoT вважається слабкою ланкою в кібербезпеці. XDR навчиться виявляти загрози цим пристроям і реагувати на них, а також керувати їх захистом з єдиної консолі.

Також важливим трендом є рух до створення «XDR під замовника», тобто підлаштованого під регуляторні вимоги конкретної галузі. Це, ймовірно, призведе до появи XDR, «заточених» під потреби різних індустрій: наприклад, сфера охорони здоров'я вимагатиме рішень, які захищають дані пацієнтів, а фінансова — які захищають банківські транзакції.

А ось прогнози від компанії Samurai Security (яка має власний продукт, SamuraiXDR). По-перше, відбувається консолідація вендорів: оскільки замовники прагнуть скоротити число постачальників і зекономити коштів (про це писав і Gartner), виробники, які додають до своїх рішень можливості XDR, матимуть перевагу. По-друге, серед пропозицій XDR домінуватимуть хмарно-нативні, оскільки вони дозволяють вирішувати питання масштабування, зокрема для захисту ресурсів у хмарних же середовищах. По-третє, ключовим чинником буде якість реакції на загрози, що залежить від «калібру» інструментів ШІ та МН. А також, у міру розростання поверхні атаки і об'єму даних, XDR повинні підтримувати низький рівень шуму, тобто зайвих сповіщень.

Є й проблеми. Род Трент, старший програмний менеджер Microsoft, відносить до них брак стандартизації і взагалі чіткого визначення, що таке XDR, так само як і чіткої методології оцінюванні продуктів. Далі: хоча концепція XDR ставить на меті інтеграцію даних з розрізнених джерел, все ще проблеми з сумісністю і взаємодією, особливо коли мова про застарілі системи. І, по-третє, оскільки XDR збирає велику кількість даних, він мусить забезпечувати цілісність і захищеність цих даних для дотримання норм відповідного законодавства на кшталт GDPR.

Проте XDR — це все ще порівняно нова ідея, яка продовжує розвиватися, тож на ці виклики буде зрештою знайдено відповіді.

Василь ТКАЧЕНКО, **МтБ**