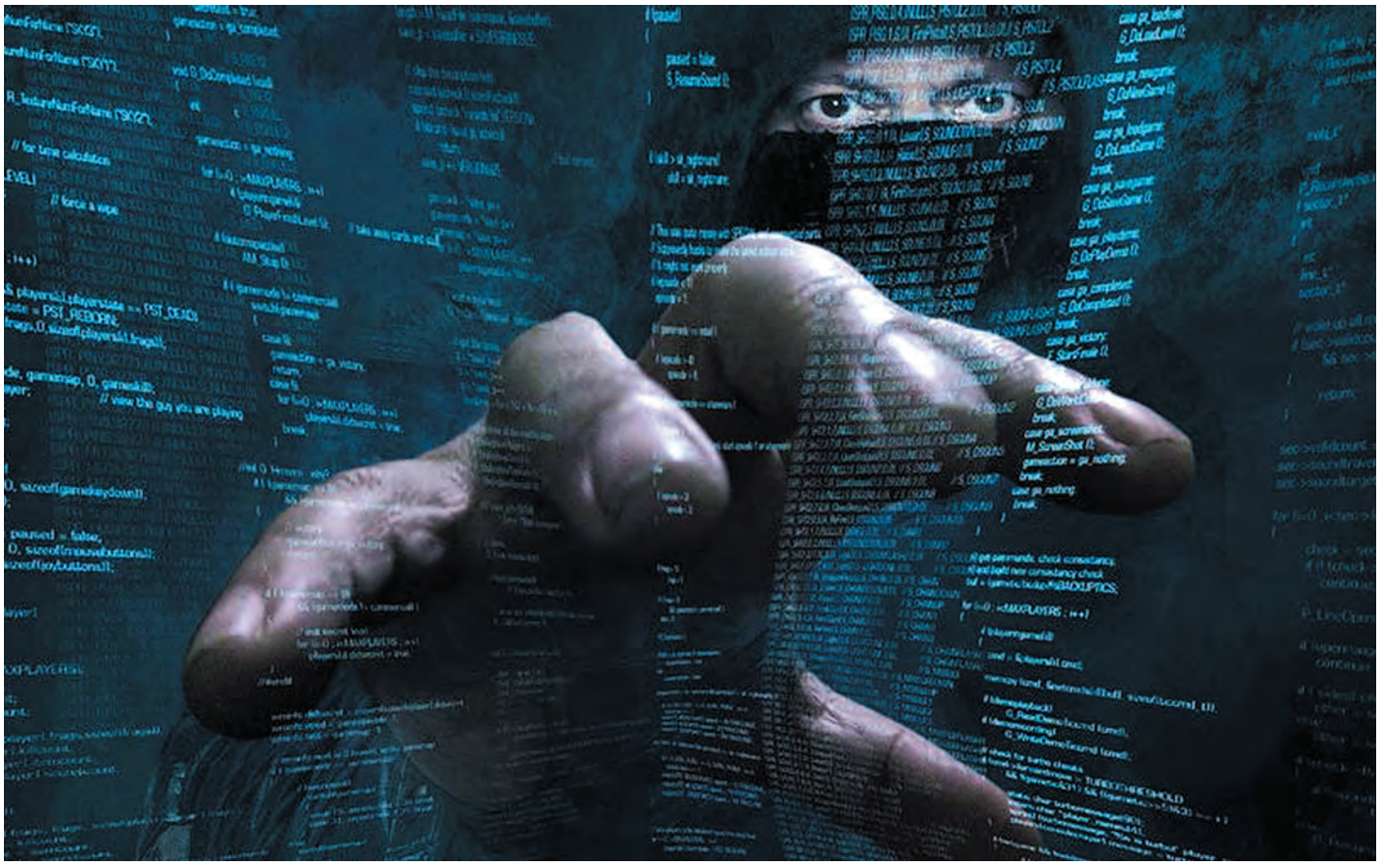
DLP як захист від цифрових несунів



Системи запобігання витокам інформації пройшли шлях від захисту електронної пошти до хмар.

Як відомо, хто володіє інформацією, той володіє світом. А хто інформацію втрачає, тому загрожує покарання відповідно до європейського регламенту захисту персональних даних (GDPR). У новинах час від часу з'являються повідомлення про багатомільйонні штрафи, сплачені компаніями, що допустили витік. Тому захист інформації від крадіжки — завдання завжди важливе.

З цією метою використовуються спеціалізовані системи запобігання витокам даних (Data Leak Prevention, DLP). Пандемія коронавірусу, що призвела до переведення співробітників на віддалену роботу, підкреслила потребу у захисті на рівні робочих станцій.

Погляньмо, як саме працюють системи DLP і які рішення представлені на українському ринку.

Захист персональних даних крокує планетою

Відтоді, як у 2016 році набув чинності стандарт GDPR, до захисту персональних даних почали ставитися значно серйозніше, і не тільки в Євросоюзі. По-перше, стандарту мусять дотримуватися будь-які компанії, які ведуть справи з громадянами ЄС. А по-друге, схоже законодавство починає потроху з'являтися в інших частинах світу.

Наприклад, наприкінці минулого року мешканці штату Каліфорнія схвалили на референдумі «Каліфорнійський акт про право на конфіденційність» (CPPA), який має набути чинності 1 січня 2023 року. Цей акт розширює існуючий закон, також прийнятий кілька років тому, та робить його більш подібним до GDPR. CPPA захищатиме таку інформацію, як ID-картки, водійські права, номери соціального страхування, банківські картки, відомості про расову приналежність, релігійні переконання, біометричні дані та ще багато чого. Серед іншого, у новому законі скасовано 30-денний термін, упродовж якого компанія повинна усунути порушення; постраждалі зможуть одразу вимагати відшкодування.

Також восени у Китаї було оприлюднено місцевий аналог GDPR — «Закон про захист особистої інформації» (PIPL). Він об'єднує існуючі закони у цій царині, вводить суворі штрафи і принцип екстериторіальності. Тоді ж перший у Латинській Америці закон про персональні дані був прийнятий у Бразилії. Загалом подібні документи перебувають на розгляді у низці країн.

Сайт *enforcementtracker.com* відстежує штрафи, сплачені відповідно

до GDPR. Найбільший, у розмірі €50 млн, було виставлено компанії ***Google*** з формулюванням «недостатні правові основи для обробки даних», а найбільший штраф за «недостатні технічні та організаційні заходи для забезпечення безпеки даних» (€22 млн) отримала ***British Airwaives***, яка у 2018 році допустила витік інформації: злочинці тоді змогли отримати доступ до майже 430 тис. клієнтів і співробітників авіакомпанії.

Загалом такі витоки здебільшого є наслідком різних кібератак; зокрема, здирники почали красти дані у своїх жертв і публікувати в Інтернеті. Проте не менш серйозною може бути загроза зсередини, з боку «зловмисних інсайдерів»: наприклад, співробітників, які чимось незадоволені або вирішили підзаробити. Навіть якщо нема поганого наміру, звичайне недбальство може призвести до того, що важлива інформація потрапить в Інтернет, на незахищену «флешку», яку можуть поцупити, або на сторонню електронну адресу. Нинішня пандемія ще більш ускладнила ситуацію, адже тепер багато хто працює вдома на особистих комп'ютерах, які контролювати ще складніше.

Торік організація ***Ponemon Institute*** повідомила, що кількість інсайдерських атак зросла за три роки на 47%: з 3200 у 2018 році до 4716 у 2020-му. А загальні збитки від цих інцидентів збільшились на 31%: з $8,76 млн до $11,45 млн. При цьому 62% інцидентів сталися через недбальство персоналу і вартували організаціям у середньому $307 тис., тоді як дії зловмисних інсайдерів обходились у $872 тис. Також повідомлялось, що в середньому на усунення інсайдерської загрози йшло 77 днів, і менше 13% вдавалося впоратися за місяць.

Унеможливити витоки даних «зсередини» покликані системи DLP.

Анатомія DLP

Аналітична компанія ***Radicati*** визначає DLP як «апаратне і програмне забезпечення, хмарні сервіси і гібридні рішення, які забезпечують нагляд за електронними даними і управління ними, допомагаючи організаціям запобігти несанкціонованому поширенню інформації». При цьому DLP-рішення повинні бути «контентно-свідомими», тобто розуміти зміст інформації і контролювати її не просто за ключовими словами, які зустрічаються в тексті. ***Gartner*** зазначає, що DLP — це насамперед добре виписаний процес, який підкріплюється допоміжними технологіями.

DLP забезпечує захист даних, які перебувають у трьох станах. Насамперед це дані, що використовуються (Data in use), тобто обробляються якоюсь програмою чи застосунком. Для цих даних потрібно вручну або автоматично встановлювати правила щодо можливих дій з ними (дозвіл на зміну, контроль друку, контроль копіювання і вставки тощо). Також задають дозволені протоколи зв'язку і типи пристроїв, за допомого яких можливий доступ до цих даних.

Дані, які знаходяться в русі (Data in motion), потрібно убезпечити від передавання за межі організації (наприклад, електронною поштою або через USB), публікування в соціальних мережах і т. ін., а також їх пересилання в незахищені сховища. Ті дані, які знаходяться на зберіганні, чи то пак у спокої (Data at rest), зокрема у хмарі, також потребують захисту від несанкціонованого доступу, у тому числі шляхом періодичного моніторингу.

Традиційно DLP-системи поділяють на дві категорії: корпоративного класу (Enterprise DLP, EDLP), або ж відокремлені (Dedicated), та інтегровані. Перші являють собою спеціалізовані рішення, другі реалізуються як функції у складі інших засобів безпеки.

Відокремлені DLP забезпечують захист даних у будь-якому стані, а також мають повний арсенал функцій для забезпечення політик захисту залежно від потреб компанії (наприклад, встановлення правил для різних груп користувачів і типів пристроїв), засоби візуалізації, сповіщення і розслідування. Вважається, що відокремлені DLP є чи не єдиним варіантом для великих компаній, але можуть бути надто дорогими й складними для менших підприємств. Інтегровані рішення дешевші і потребують менше часу для розгортання, проте мають більш обмежені можливості настроювання, управління і візуалізації. Gartner зазначає, що інтегровані DLP купують організації, які потребують лише базової функціональності або захисту конкретного напряму — наприклад, електронної пошти. Ті ж, яких цікавить захист кількох напрямів (наприклад, кінцевих пристроїв, пошти і хмари), встановлюють рішення корпоративного класу. Проте малим і середнім бізнесам часто важко впроваджувати й експлуатувати такі системи і при цьому отримувати помітний результат.

Radicati пропонує поділ рішень на три типи.

Повноцінні DLP, власне, захищають дані у всіх трьох станах і, окрім ключових слів, беруть до уваги метадані, роль співробітника в організації, належність даних та інші параметри, які визначають їхню цінність. За допомогою цих рішень можна програмувати різні методи реагування на спробу витоку (блокування, попередження, переміщення до карантину тощо).

Одноканальні DLP-рішення (Channel DLP) забезпечують захист даних в якомусь одному стані (зазвичай у русі) по одному з каналів передавання (наприклад, електронною поштою), вони враховують контент, але найчастіше здійснюють блокування лише за ключовими словами.

Нарешті, полегшені **рішення DLP-Lite** є додатками до інших систем (наприклад, архівування та зберігання інформації), не завжди враховують контент і зазвичай відстежують лише дані, що знаходяться на зберіганні або використовуються.

Зазвичай DLP складається з декількох модулів, які відповідають за захист усіх трьох типів даних. Наприклад, контроль інформації, яка знаходиться в русі, можуть забезпечувати окремі компоненти для знімних носіїв, електронної пошти, хмарних сервісів. Окремий модуль займається пошуком чутливих даних у сховищах. Деякі платформи працюють лише на кінцевих пристроях, де їхні програмні агенти слідкують за усіма операціями з даними, інші мають можливості для відстеження інформації, яка передається в мережі

СПІВРОБІТНИКИ ПОБОЮЮТЬСЯ ЗА СВОЇ ДАНІ

Згідно з дослідженням Cisco 2021 Data Privacy Benchmark Study, через пандемію люди зіткнулися з тим, що від них очікують, а то й вимагають надання персональної інформації для боротьби з поширенням COVID-19. При цьому значна частина діяльності перемістилася в Інтернет, що ставить чимало запитань, пов'язаних з конфіденційністю.

Зокрема, серед опитаних 4400 фахівців з безпеки, які представляли 25 країн, 60% відповіли, що виявилися не готовими забезпечити вимоги щодо безпеки й конфіденційності даних при переході на віддалену роботу, 87% висловили стурбованість щодо рівня захищеності даних в інструментах віддаленої роботи. В той же час 57% респондентів підтримують використання особистих даних роботодавцями задля підвищення безпечності робочих місць, хоча надавати інформацію про місцезнаходження, контакти, інформацію про зараження готові менше половини опитаних.

Загалом 75% організацій вважають, що інвестиції в захист персональних даних вигідні з точки зору пом'якшення шкоди безпеці, підвищення маневреності, інноваційності та операційної ефективності, а також для підсилення лояльності й довіри споживачів. При цьому більше третини організацій вже отримують вигоду, яка щонайменше удвічі перевищує витрати.

і назовні. Реалізація DLP також можлива у різних варіантах: як апаратне рішення, віртуальний пристрій або з розміщенням у хмарі.

DLP плюс

Gartner у 2017 році припинив публікувати «магічний квадрант» EDLP, наголосивши, що цей ринок вже є зрілим, і продуктивність представлених на ньому рішень вийшла на плато.

У квітні 2018 року, власне три роки тому, аналітик Gartner Авіва Літан опублікувала допис, у якому фактично стверджувалося, що «DLP вмирає». Той допис викликав бурхливу дискусію, після чого його було видалено й переписано, тож уявити його зміст можна лише з відгуків, десь як втрачені тексти античних авторів. Проте йшлося, очевидно, про те, що DLP не забезпечують належного захисту в умовах, коли «периметр» фактично розчинився, а більшість загроз надходить з кінцевих пристроїв. І тому сучасні DLP повинні інтегруватися з рішеннями, які забезпечують захист термінального обладнання (EDR) і контроль за поведінкою користувачів.

Власне, цьому було присвячено оновлений допис Авіви Літан, де вона навела класи рішень, які можуть допомогти у боротьбі з інсайдерськими загрозами. По-перше, це UEBA (аналітика поведінки користувачів і об'єктів). Ці системи займаються профілюванням користувачів, груп і різних сутностей, завдяки чому надалі визначають аномальні дії чи транзакції (наприклад, підозрілий вхід у мережу). Іншим конкурентом DLP є системи моніторингу персоналу — рішення агентного типу, які забезпечують повну видимість дій працівника у мережі організації (зокрема, операції копіювання і вставки, яких не бачить UEBA). А системи датацентричного аудиту і захисту (DCAP) відслідковують і аналізують привілеї користувачів і адміністраторів, а також спроби доступу до даних.

В рамках заочної дискусії один з виробників, GTB Technologies (віднесений Gartner до візіонерів), натякнув на упередженість Gartner через зарахування до лідерів одного з конкурентів (вочевидь, Digital Guardian), бо той оголосив, що «застарілі DLP-рішення мало що дають», і додав у свою платформу функціональність EDR та UEBA. А це, мовляв, було рівнозначно визнанню, що їхня базова DLP-система вийшла невдалою.

Дійсно, Gartner відзначає, що виробники DLP-систем впроваджують технічні рішення на кшталт EDR, які здатні швидко виявляти зловмисну діяльність на кінцевому пристрої. Завдяки цьому правилу DLP можуть діяти з урахуванням контексту. Наприклад, DLP може показувати певну операцію з даними як малозначущу подію, проте зіставлення з інформацією від робочої станції, де знайдено шкідливе ПЗ або недовірений процес, дозволить ідентифікувати подію як спробу виведення даних назовні. Подібним чином інтеграція з UEBA забезпечує більш точну оцінку подій або виявлення закономірностей на основі даних про поведінку інсайдерів. Наприклад, рівень серйозності події, зафіксованої DLP, може бути підвищено у разі входів у систему з різних місць, доступу до застосунків у нетиповий час або спроб отримати більше даних, ніж зазвичай.

Ринок DLP та його учасники

Агенція Mordor Intelligence оцінює світовий ринок DLP 2020 року у $1,21 млрд і прогнозує, що до 2026-го він досягне $3,75 млрд при середньорічному темпі зростання на рівні 23,59%. Radicati оцінювала ринок DLP 2019 року у $1,2 млрд і прогнозувала, що у 2023-му він становитиме $2,3 млрд.

Станом на середину 2017 року, коли Gartner видав свій останній Magic Quadrant для EDLP, до числа лідерів (за інтегральними показниками глибини бачення і спроможності забезпечення) увійшли ***Symantec*** (зараз ***Broadcom***), ***Digital Guardian***, ***Forcepoint*** та ***Intel Security*** (тепер ***McAfee***).

Radicati Group публікує схожі «квадранти» за іншими критеріями: функціональністю і стратегічним баченням. Відповідно учасники ринку поділені на першопрохідців, спеціалістів (це або нові учасники, або усталені компанії з давніми клієнтами, які всім задоволені), зрілі гравці, які дещо сповільнили інновації, а врешті топ-гравці, які наразі і є лідерами ринку. До таких, відповідно до дослідження 2019 року, віднесені Symantec, Digital Guardian і McAfee, тоді як Forcepoint визнано зрілим гравцем.

Системи DLP, які можна зустріти в Україні, виробники цих систем та їхні місцеві партнери наведені в **таблиці.** Тут не розглядаються інтегровані модулі DLP, які входять до складу інших платформ захисту, як-от інтернет-шлюзи або мережеві екрани (такі є, наприклад, у ***Palo Alto***, ***Trend Micro*** і багатьох інших виробників).

Далі розповімо про деякі з цих DLP-рішень.

Таблиця. Основні виробники DLP та їх партнери в Україні

Виробник	Країна	Назва продукту або лінійки	Дистриб'ютори в Україні	Партнери в Україні
Acronis	Сінгапур/ Швейцарія	DeviceLock	SoftiCo	
Broadcom (Symantec)	США	Symantec Dala Loss Prevention	Світ IT	
CoSoSys	Румунія	Endpoint Protector	CoreWin	
Digital Guardian	США	Digital Guardian	БАКОТЕК	
Forcepoint	США	Forcepoint DLP	Softprom	IBM Україна, Intrasystems, ISSP
McAfee	США	Total Protection for DLP	БАКОТЕК	GigaSafe, ITIS, Netwave, Optidata, Softlist, SoftwareOne Ukraine
Safetica	Чехія	Safetica	Adeon SK (дистриб'ютор ESET)	

Broadcom (Symantec)

Symantec у 2019 році продала свій бізнес корпоративної безпеки компанії Broadcom. Остання зберегла бренд Symantec, під яким і пропонує DLP-системи.

Лінійка включає в себе рішення для різних застосувань. Symantec DLP Endpoint, як видно з назви, забезпечує захист даних на робочих станціях. За це відповідає агент, який складається з двох модулів: Discover і Prevent. Перший сканує локальні диски, виявляє чутливі файли і вживає заходів (шифрування, відправлення на карантин тощо). Другий стежить за діями користувачів і реагує на них, а також попереджає про недозволені операції за допомогою спливаючих вікон або поштою. При цьому користувачі мають можливість надати пояснення своїм діям або скасувати їх.

Рішення Symantec DLP for Networks відстежує рух файлів, які передаються за допомогою мережевих протоколів. Зокрема, компонент DLP Network Monitor аналізує вихідний трафік за допомогою глибокої перевірки пакетів (DPI). DLP Network Prevent for Email контролює повідомлення електронної пошти і може їх змінювати, перенаправляти або блокувати. Аналогічно DLP Network Prevent for Web моніторить веб-трафік і може блокувати запити або видаляти чутливий контент. Усі три модулі розташовуються на вихідних точках мережі.

Для захисту даних, які зберігаються, виробник пропонує рішення Symantec DLP for Storage. Воно складається з двох компонентів: Symantec DLP Network Discover та Symantec DLP Network Protect. Перший розшукує конфіденційні дані, скануючи файлообмінники, бази даних та інші сховища, а другий захищає знайдені вразливі файли, наприклад, шляхом шифрування, переміщення або направлення в карантин. При цьому на місці вилученого файлу залишається текстовий документ з відомостями про те, чому саме його було переміщено.

Також виробник може запропонувати два рішення, які захищають дані у хмарі. Symantec DLP Cloud Detection Service інспектує контент, який передається через хмарні застосунки і веб-трафік, і автоматично реагує відповідно до запроваджених політик. Рішення інтегрується з брокером хмарного доступу Symantec CloudSOC, що дозволяє захищати дані у різноманітних застосунках, таких як Office 365 і Dropbox. Symantec DLP Cloud Service for Email здійснює моніторинг і захист трафіку корпоративної пошти через такі сервіси, як Gmail for Work, Microsoft Office 365 Exchange Online та Microsoft Exchange Server.

У версії DLP 15.5, серед іншого, впроваджено інтеграцію з системою захисту кінцевих точок Symantec Endpoint Protection (SEP). Це дозволяє запобігати витокам даних через зловмисні або невідомі застосунки: керуючись репутаційною базою, агент SEP може звеліти агентові DLP стежити за підозрілою програмою, завдяки цьому DLP фіксуватиме спроби доступу до важливих файлів і блокуватиме їхню крадіжку. Виробник також пропонує інтеграцію DLP з UEBA-системою Symantec ICA, що дозволяє вдосконалити пріоритезацію подій (виявляти ті, які становлять справжню небезпеку) і шукати зловмисних інсайдерів.

Digital Guardian

Ця компанія пропонує DLP за моделлю SaaS на базі AWS. Архітектура платформи складається з трьох основних компонентів: сенсорів, функціональних модулів і хмарної інфраструктури (**рис. 1**).

Сенсорами Digital Guardian є, насамперед, агенти, які працюють автономно на рівні ядра операційної системи, що забезпечує видимість усіх операцій з даними і контроль доступу до пристроїв введення/виведення. Агенти відслідковують усі звернення і можуть втрутитися у разі порушення політики безпеки (наприклад, заблокувати дію або попросити

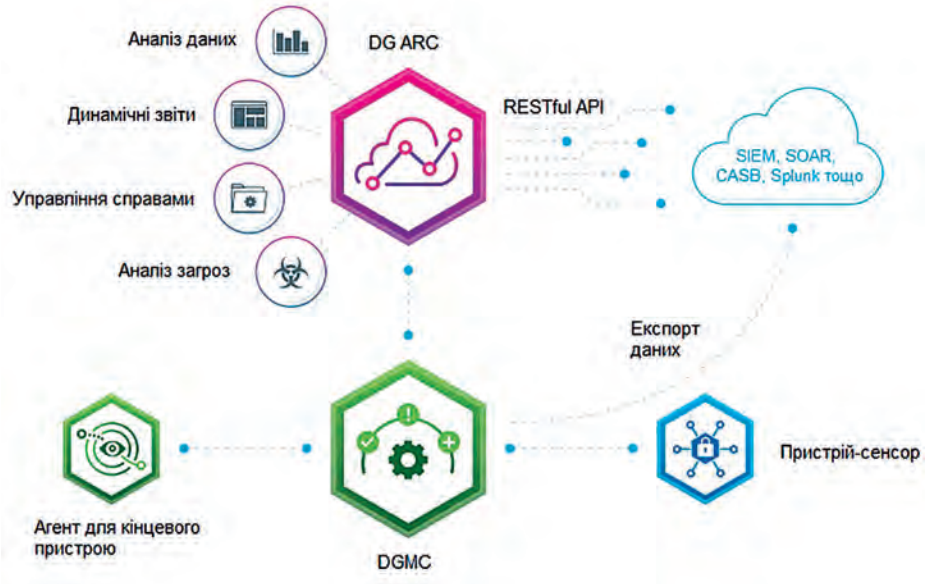


Рис. 1. Архітектура Digital Guardian

користувача скасувати її чи пояснити). Агенти здійснюють моніторинг самих себе для захисту від спроб зловмисників завершити процес або вставити шкідливий код. У разі порушення роботи запускається новий агент. Також програма може працювати у прихованому режимі, коли вона не відображається у менеджері завдань і подібних застосунках, а файли і папки агента не «світяться» у файловій системі. В Digital Guardian інтегровано і функціональність EDR, яку забезпечує той самий DLP-агент.

Іншим видом сенсора є пристрій (Appliance), який контролює мережевий трафік: поштовий, HTTP, FTP, SSL тощо, а також дозволяє виявляти чутливу інформацію, що зберігається в базах даних, сховищах і хмарах.

Розширені можливості захисту забезпечують модулі Digital Guardian. Це, зокрема, хмарний сервіс DG Analytics & Reporting Cloud (ARC), який здійснює контекстний аналіз, виявлення аномалій за допомогою статистичних моделей і машинного навчання, а також відображення даних. Власне, в цьому і полягає SaaS-модель: збереження і обробка даних відбуваються у хмарі. З консолі управління (DGMC) здійснюється конфігурування системи, запуск агентів і поширення політик. Застосунок Data Discovery автоматично сканує локальні й мережеві файлосховища, надсилаючи сповіщення про виявлені проблеми з детальним переліком файлів, їх місцезнаходжень і конкретних порушених правил. Data Classification у реальному часі здійснює класифікацію файлів після їх виявлення, створення, переміщення і т.д., використовуючи задані критерії (наприклад, за ключовими словами або місцем зберігання). Ця класифікація потім додається до сповіщень про інциденти.

McAfee

Платформа цього виробника носить назву Total Protection for DLP. Як і інші подібні рішення, вона складається з декількох компонентів, а налаштування здійснюється з єдиної панелі ePolicy Orchestrator.

McAfee Data Loss Prevention Endpoint забезпечує захист інформації на кінцевих пристроях і у хмарі. Рішення саме по собі здійснює контроль різних каналів, у тому числі знімних носіїв, електронної пошти, месенджерів, буфера обміну тощо. Рішення інтегроване з системою захисту даних у хмарі MVISION Cloud, завдяки якому можна поширити дію локальних політик DLP на хмарне середовище. Також є інтеграція зі сторонніми системами UEBA, що дозволяє виявляти дивну і потенційно небезпечну поведінку користувачів. Є можливість присвоєння даним, що передаються, міток Microsoft Azure (Azure Information Protection) і подальшого розпізнавання файлів з цими мітками. При цьому користувачі можуть вручну класифікувати документи і самостійно запускати сканування мережі. Управління системою здійснюється через хмарну консоль.

McAfee DLP Prevent — це засіб застосування політики захисту до різноманітної вихідної інформації (загалом понад 300 видів контенту). Для цього використовується той самий модуль класифікації, що й в DLP Endpoint. Інтеграція з проксі-сервером і агентом доставки повідомлень (MTA) дозволяє блокувати пересилання на рівні застосунків. Також можливий моніторинг електронної пошти на мобільних пристроях, при цьому встановлення агента на термінал не потрібно.

За пошук і класифікацію даних на зберіганні відповідає рішення McAfee DLP Discover, яке працює як локально, так і у хмарних середовищах. Загалом воно може автоматично перевіряти усі доступні ресурси на предмет порушення політик і генерувати сповіщення. Функція точного зіставлення даних (Exact Data matching) дозволяє ідентифікувати великі об'єми даних за їх фрагментами, а функція оптичного розпізнавання символів захищає текст у відсканованих зображеннях. McAfee Device Control запобігає несанкціонованому використанню знімних пристроїв: зокрема, виконуючи їх блокування, захист доступу до файлів, моніторинг документів «лише для читання» і сповіщення про дії користувача на таких пристроях.

Також до складу платформи входить рішення для контролю даних, що передаються мережею — McAfee DLP Monitor. Воно сканує трафік у режимі реального часу, перевіряючи документи на основі 150 готових правил, проводить класифікацію цих документів і зберігає отриману інформацію у пропрієтарній базі даних. За допомогою пошукового інтерфейсу можна бачити, хто й куди пересилає інформацію, це допомагає адміністраторам прописувати правила і зменшує кількість хибно позитивних сповіщень.

CoSoSys

Румунського виробника CoSoSys Gartner відносить до нішових гравців, а Radicati — до першопрохідців. Його платформа Endpoint Protection складається з чотирьох модулів, які можна комбінувати відповідно до потреб замовника (**рис. 2**). Є три варіанти реалізації: у хмарі, як апаратний або віртуальний пристрій. Цікаво, що компанія пропонує своє рішення як заміну Symantec DLP.

Першим рівнем захисту є Device Control — модуль, який контролює

Рис. 2. Функціональні модулі CoSoSys Endpoint Protection та їх можливості

доступ до пристроїв USB і периферійних портів. Захист можна посилити за допомогою модуля Enforced Encryption, який шифрує усі дані, що записуються на пристрій. Модуль Content-Aware Protection контролює усі дані, які полишають організацію (будь то через USB, пошту, месенджери абощо), для чого використовується як контентний, так і контекстний аналіз, а також DPI. Модуль sDiscovery шукає чутливі дані, які зберігаються на пристроях користувачів, при цьому можуть застосовуватись як чорні списки з конкретними критеріями пошуку (тип файла, ключові слова тощо), так і білі, які виключають зі сканування рисунки, відео і подібний контент, тим самим скорочуючи процес.

Acronis

Acronis нема в рейтингах Gartner і Radicati. У липні 2020 року Acronis придбала DeviceLock — російську компанію, що спеціалізувалася на запобіганні витокам даних на кінцевих пристроях — і відтоді продовжує розвивати рішення, а також інтегрувати функції DeviceLock у власний продукт. Рішення є термінальним — агенти DeviceLock працюють на кінцевих пристроях, де й відбувається контроль. Нещодавно виробник провів кілька вебінарів, присвячених цим рішенням, спільно з дистриб'ютором в Україні – SoftiCo.

DeviceLock забезпечує контроль різних видів пристроїв та інтерфейсів, а також каналів комунікацій, включно з месенджерами. При цьому здійснюється контекстна перевірка (права користувача, час, джерело та напрям передачі тощо), яка супроводжується контентною фільтрацією в режимі реального часу. На основі цих даних система приймає рішення про дозвіл або блокування. Наприклад, доступ у Facebook буде перекрито у разі спроби викладання туди інформації, яка захищається.

Контентна фільтрація включає перевірку тексту за ключовими словами з використанням морфологічного аналізу і транслітерації, шаблонів, залученням специфічних словників, звірянням «цифрових відбитків». Наприклад, можна заблокувати передавання файлу електронною поштою, якщо в ньому зустрічаються паспортні дані.

Якщо служба безпеки боїться порушення бізнес-процесів через блокування або просто не готова обмежувати співробітників, DLP може здійснювати моніторинг подій: протоколювання, тіньове копіювання усіх даних, переданих по каналах, які захищаються, а у версії 9.0 буде додано моніторинг активності користувачів. Також підтримується запис екрану і клавіатурного вводу для подальшого аналізу, тригерами для якого можуть бути, наприклад, підключення знімного носія, спроба передавання файлів зі специфічним вмістом тощо. Запис спрощує подальше розслідування інцидентів; окрім того, якщо працівники ознайомлені з такою політикою, це суттєво зменшує ризик витоків.

Також DeviceLock здійснює сканування даних, що зберігаються, і автоматично усуває порушення політики безпечного зберігання: видаляє, шифрує або переміщує документи, знайдені в неналежних місцях, або ж змінює права доступу до них. Це може здійснюватись у ручному режимі або за розкладом.

Про зафіксовані події система попереджає адміністраторів. Є можливість повнотекстового пошуку в тіньових копіях в централізованому або розподіленому архіві, а також автоматичного пошуку за розкладом. А нова функція — «Досьє користувача» — дозволяє бачити всю зведену інформацію щодо поведінки співробітника і його «індикатор лояльності».

Одним з варіантів організації віддаленої роботи є підключення з дому до робочого комп'ютера або віртуалізованого робочого середовища, використовуючи власний пристрій. Цей сценарій не надто відрізняється від концепції BYOD, якій вже навчилися давати раду. У Acronis на цей випадок є рішення DeviceLock Virtual DLP, яке забезпечує захист термінальних сесій, контролює буфер обміну і виявляє спроби скопіювати з корпоративного середовища важливі документи. При цьому на особистий пристрій користувача встановлюється лише застосунок для підключення, а агент DLP працює віртуально у корпоративному середовищі.

Захист даних в часи пандемії

Загалом, якщо вести мову про віддалену роботу, то проблеми з запобіганням витокам проявилися вже в перші п'ять днів пандемії, пише оглядач Девід Балан в канадському виданні IT World. Спеціалістам з кібербезпеки довелося мати справу з силою-силенною нових каналів обміну. Наприклад, аби не гаяти час, поки IT-департамент налагодить віддалений доступ, співробітники почали замість корпоративних сховищ використовувати хмарні сервіси на кшталт Dropbox і Google Drive, пересилати дані через особисту пошту і відкриті файлообмінники. Також співробітники почали активніше копіювати дані на знімні носії.

Зазнали змін і традиційні, добре відпрацьовані бізнес-процеси. Наприклад, DLP-системи зафіксували різке зростання кількості даних, які зберігалися на робочих станціях і пересилалися між ними: якщо раніше працівник міг просто підійти до колеги зі своїм ноутбуком, то тепер вони змушені спілкуватися через Інтернет. Під час відеоконференцій активно використовується режим показу екрану, і будь-хто з учасників може робити знімки інформації, яка там відображається.

Далеко не всі організації видали співробітникам робочі ноутбуки, через що ризики значно зросли, адже на приватних пристроях нема корпоративних засобів захисту, а іноді нема й бодай навіть антивірусу. На додачу особисті ПК можуть використовуватися кількома членами родини.

У той же час, пише оглядач, DLP-системи мають достатній набір можливостей для запобігання витокам конфіденційної інформації під час віддаленої роботи і, понад те, здатні контролювати поведінку користувачів. Наприклад, вони можуть відстежувати набір на клавіатурі і рухи миші, веб-серфінг, аудіо– і відеопотоки, час закриття кришки ноутбука.

А загалом перехід на віддалену роботу виявився простішим для тих компаній, які вже мали DLP-системи; тим, кому довелось вирішувати проблему з нуля, було значно важче.

Василь ТКАЧЕНКО,
Мережі та Бізнес