OMÓWIENIE ROZWIĄZANIA

Zapobieganie utracie danych za pomocą rozwiązania Fortinet FortiDLP

Streszczenie

W obliczu dużej złożoności obecnych środowisk IT, nowych przepisów dotyczących danych wrażliwych oraz istnej eksplozji danych związanych z cyfrową własnością intelektualną, wprowadzaniem pracy hybrydowej i powrotów do biura, a także prywatnymi aplikacjami pracowników i nieautoryzowanym korzystaniem ze sztucznej inteligencji (AI), ochrona danych jest obecnie trudniejsza niż kiedykolwiek dotąd. Niestety dotychczas używane programy do ochrony danych i tradycyjne, starsze narzędzia DLP nie potrafią ograniczyć ryzyka ani skutecznie chronić danych. Zapobieganie utracie danych wymaga obecnie nowoczesnego podejścia obejmującego wiele platform.

FortiDLP to chmurowe, wyposażone w funkcje AI rozwiązanie nowej generacji do ochrony danych, które pomaga zespołom ds. bezpieczeństwa przewidywać i blokować wycieki danych, wykrywać zagrożenia wewnętrzne związane z różnymi zachowaniami i uczyć pracowników właściwej higieny cybernetycznej w punkcie dostępu do danych wrażliwych. FortiDLP ułatwia zapobieganie utracie danych, zapewnia natychmiastowy wgląd w dane, pozyskuje informacje o przepływach danych biznesowych, wspomaga priorytetowe dochodzenia w sprawie incydentów oraz wykrywa aktywność o wysokim poziomie ryzyka na poziomie użytkowników, punktów końcowych i dysków w chmurze.

Do 2027 roku 70% organizacji połączy DLP i zarządzanie ryzykiem wewnętrznym z kontekstem IAM, aby skuteczniej identyfikować podejrzane zachowania[1].

Trudności z dbaniem o bezpieczeństwo danych

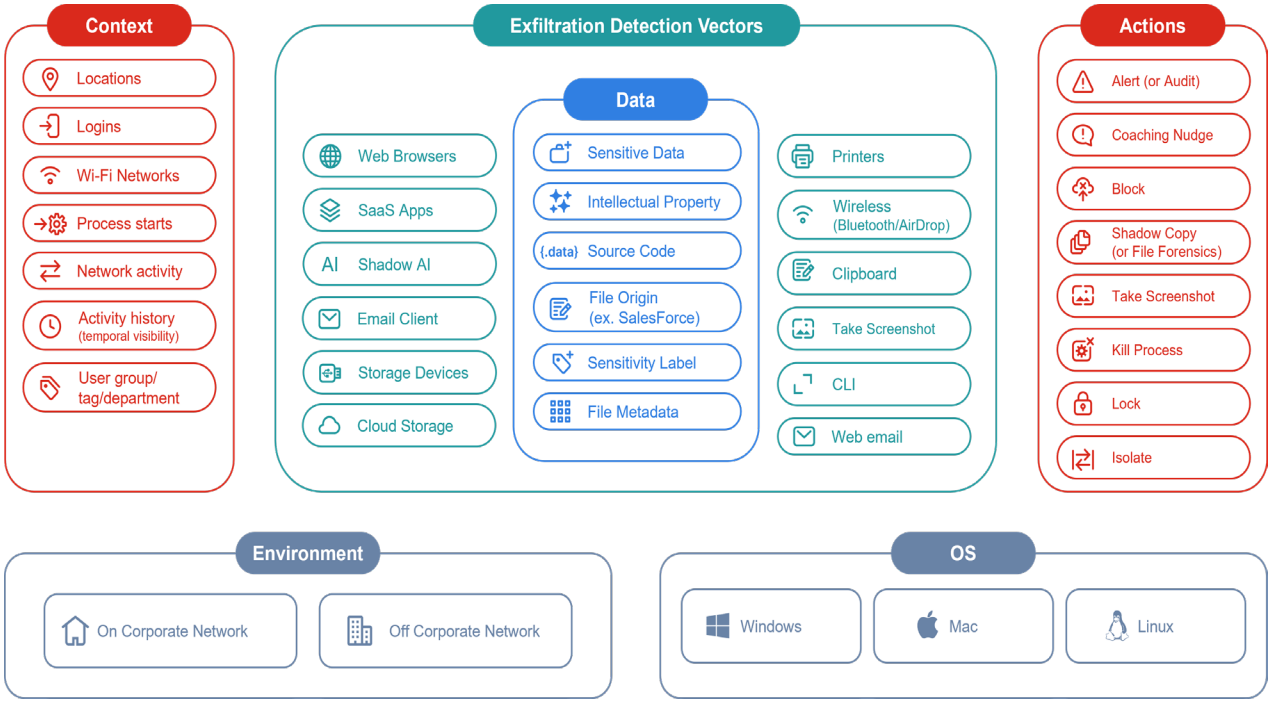
Choć wiele organizacji ma programy oraz rozwiązania DLP, dyrektorzy ds. bezpieczeństwa systemów informatycznych (Chief Information Security Officer, CISO) i liderzy ds. bezpieczeństwa znów głowią się wraz ze swoimi zespołami nad tym, jak zapewnić bezpieczeństwo danych bez szkodzenia operacjom biznesowym i obniżania wydajności pracy. Organizacje potrzebują rozwiązania, które:

- zapobiega nieautoryzowanemu przekazywaniu danych wrażliwych poza organizację bez względu na punkty takich wycieków — pocztę e-mail, chmurę, urządzenia fizyczne czy inne;
- identyfikuje i neutralizuje zagrożenia stwarzane przez mające złe zamiary osoby z firmy, które mogą mieć dostęp do danych wrażliwych;
- rozwiązuje problem korzystania z autoryzowanych i nieautoryzowanych aplikacji oraz usług w chmurze, które mogą zwiększać ryzyko naruszenia danych;
- umożliwia pracownikom bezpieczne korzystanie z publicznie dostępnych narzędzi generatywnej AI, takich jak OpenAI ChatGPT czy Google Gemini;
- upraszcza wdrażanie rozwiązań DLP i zarządzanie nimi, eliminując zapotrzebowanie na rozbudowaną infrastrukturę IT i korzystanie z gotowych polityk.

Ujednolicone podejście do ochrony danych

FortiDLP stosuje nowoczesne i ujednolicone podejście do ochrony danych, łącząc DLP, zarządzanie zagrożeniami wewnętrznymi, zabezpieczenia danych SaaS, analizy zachowań i szkolenie użytkowników w zakresie ryzyka. W odróżnieniu od tradycyjnych podejść FortiDLP nie wymaga infrastruktury IT, męczącego wykrywania i klasyfikowania danych ani gotowych polityk.

Chmurowa technologia FortiDLP oznacza, że rozwiązanie to można wdrożyć w kilka minut — za pomocą zaawansowanego agenta i konektorów — i jeszcze tego samego dnia zyskać wgląd w przepływy danych biznesowych oraz ochronę danych. Lekka, skalowalna technologia agentów w FortiDLP odpowiada za kontrolowanie treści i danych w ruchu. Po wdrożeniu agenta i konektorów SaaS rozwiązanie FortiDLP „widzi” interakcje między użytkownikami, zespołami oraz danymi i nie potrzebuje do tego funkcji wykrywania, etykietowania ani polityk.



Ilustracja 1. Zasady działania FortiDLP

FortiDLP stosuje zintegrowane z agentem uczenie maszynowe w celu ustalenia poziomu odniesienia aktywności. Następnie za pomocą algorytmów do analizy zachowań oraz funkcji kontroli na poziomie kontekstu i treści ustala typowe zachowania, a także zachowania niespotykane wcześniej, czyli odbiegające od normy. Na podstawie tych informacji analitycy incydentów mogą nadawać priorytet dochodzeniom w sprawie zaobserwowanej aktywności o wysokim poziomie ryzyka lub budzącej podejrzenia.

FortiDLP obejmuje asystenta AI, który zestawia dane związane z aktywnością o wysokim poziomie ryzyka i ustala ich konteksty, aby przyspieszyć analizy incydentów za pomocą działań zamapowanych na bazę wiedzy MITRE Engenuity™ Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base. Ponieważ FortiDLP jest natywnym rozwiązaniem chmurowym, organizacje mogą aktywować usługi i uzyskiwać obraz ryzyka związanego z danymi w ciągu kilku minut — a dzięki temu chronić dane wrażliwe. Ponadto rozwiązanie to:

Dane są obecnie wyjątkowo mocno zagrożone. W 2024 roku średni koszt złamania zabezpieczeń danych wynosił 4,88 miliona dolarów, a zatem o 10% więcej niż w roku 2023[2].

- monitoruje korzystanie z aplikacji w modelu SaaS, w tym nieautoryzowanych narzędzi AI, na przykład generatywnej AI, a jednocześnie szkoli użytkowników w zakresie ryzyka w punkcie dostępu do danych wrażliwych;
- udostępnia aktualną konsolę zarządzania i system analiz zachowań umożliwiające monitorowanie, raportowanie i zautomatyzowane działania;
- zapewnia natychmiastowy wgląd w ruch danych bez stosowania jakichkolwiek polityk;
- trafnie wykrywa własność intelektualną i dane wrażliwe przy użyciu zaawansowanej klasyfikacji danych, pochodzenia danych i śledzenia danych opartego na tożsamościach;
- zapewnia kontrolę zgodności z przepisami, obejmującą zapobieganie utracie danych przy minimalnym wysiłku dzięki szablonom polityk dotyczących danych osobowych, chronionych informacji dotyczących zdrowia i danych kart płatniczych.

Rozwiązanie nowej generacji do zapobiegania utracie danych

FortiDLP oferuje dogłębny wgląd w dane, oceny ryzyka oraz polityki ochrony danych, wspomagając dbanie o bezpieczeństwo krytycznych zasobów informacyjnych w sieci i poza nią. FortiDLP analizuje, które dane i jak są wykorzystywane, oraz umożliwia ustalanie najlepszych reakcji. FortiDLP:

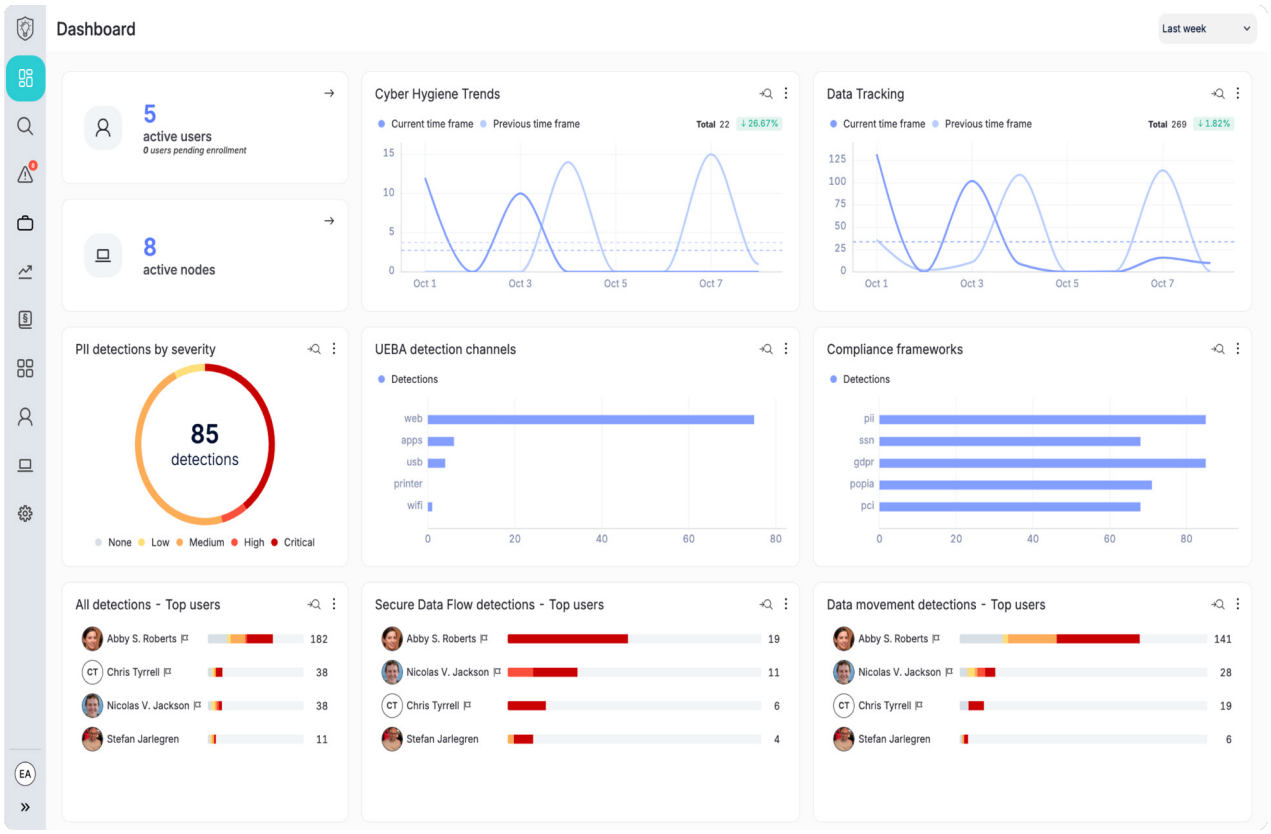
- zapobiega utracie danych wskutek ich celowego lub przypadkowego wyprowadzenia na zewnątrz;
- monitoruje zagrożenia wewnętrzne i pracowników wysokiego ryzyka;
- chroni dane używane przez aplikacje SaaS i inne;

- stosuje analizy zachowań użytkowników i jednostek na dużą skalę;
- szkoli użytkowników w punkcie dostępu do danych wrażliwych w zakresie właściwego obchodzenia się z danymi;
- identyfikuje nieautoryzowane korzystanie z AI i blokuje wysyłanie do niej danych wrażliwych.

FortiDLP nie potrzebuje predefiniowanych polityk. Klasyfikuje i śledzi dane w czasie rzeczywistym, zapewniając natychmiastowy wgląd oraz ochronę danych. Bez względu na to, czy dana organizacja korzysta z danych ustrukturyzowanych, czy nieustrukturyzowanych, FortiDLP może je śledzić i podejmować kroki w celu ich ochrony.

FortiDLP automatycznie gromadzi, uzupełnia i indeksuje dane o aktywności w kontekście różnego typu zdarzeń, takich jak uwierzytelnianie, działania związane ze stronami internetowymi, pocztą e-mail, aplikacjami i nośnikami USB oraz tworzenie, udostępnianie i pobieranie plików. Taki zestaw danych służy do następujących celów:

- naświetlanie i raportowanie ruchu danych oraz związanych z nimi zagrożeń;
- tworzenie polityk ochrony danych;
- udostępnianie bogatych informacji o aktywności w celu wsparcia dochodzeń analityków.



Ilustracja 2. Wgląd FortiDLP w przepływy danych i ewentualne ryzyko

Zagrożenia wewnętrzne

Kanał aktywności w rozwiązaniu FortiDLP stanowi kompleksowy, usprawniony i uporządkowany chronologicznie obraz aktywności użytkowników, danych i urządzeń przed incydentem, w jego trakcie oraz po nim. Wykryte działania wysokiego ryzyka są mapowane na macierz MITRE ATT&CK i automatycznie sekwencjonowane w incydenty z oceną ryzyka w celu ułatwienia analitykom ustalania priorytetów dochodzeń.

Bezpieczny przepływ danych

Funkcja bezpiecznego przepływu danych monitoruje i śledzi ruch plików na poziomie zarządzanych punktów końcowych i aplikacji w chmurze, aby chronić dane na podstawie ich pochodzenia. Pełna historia wędrówki danych — m.in. skąd pochodzą, gdzie się znajdowały i znajdują, kto się nimi zajmował i co się z nimi działo — są mapowane na bazę wiedzy MITRE Insider Threat Knowledge Base, co przyspiesza operacje ochrony i reagowanie na incydenty.

Szkolenie w zakresie ryzyka

Funkcja szkolenia w zakresie ryzyka, bazująca na wykrywanych niedozwolonych zachowaniach, uczy pracowników podejmowania właściwych decyzji. Sprzyja to przestrzeganiu firmowych polityk bezpieczeństwa i utrzymywaniu dobrej higieny cybernetycznej.

Bezpieczeństwo danych w modelu SaaS

FortiDLP zapewnia pełny wgląd w interakcje użytkowników z danymi w chmurze i podtrzymuje ochronę, gdy dane opuszczają chmurę. Taki wgląd w interakcje pomaga zadbać o stałą ochronę poufnych informacji, bez względu na ich lokalizację czy metodę uzyskiwania do nich dostępu.

Nieautoryzowane korzystanie z AI

Administratorzy mogą konfigurować polityki dotyczące nieautoryzowanego korzystania z AI, które zapewnią równowagę między dostępem do ułatwień zwiększających produktywność a przestrzeganiem pracowników przed udostępnianiem danych wrażliwych.

Ochrona danych i ograniczanie ryzyka

Organizacje mierzą się z niespotykanymi wcześniej wyzwaniami dotyczącymi ochrony danych wrażliwych. Tradycyjne metody zapobiegania utracie danych okazują się nieskuteczne w obliczu rozwoju pracy zdalnej, wdrożeń chmur i powszechnością urządzeń niezarządzanych. FortiDLP, chmurowa technologia DLP nowej generacji przeznaczona dla punktów końcowych, oferuje kompleksowe rozwiązanie tych problemów, udostępniając narzędzia potrzebne organizacjom do ochrony danych i ograniczania ryzyka.

[1] Gartner, Gartner Unveils Top Eight Cybersecurity Predictions for 2024 (Gartner przedstawia osiem najważniejszych prognoz dotyczących cyberbezpieczeństwa na rok 2024), 18 marca 2024 r.

[2] IBM and Ponemon Institute, Cost of a Data Breach Report 2024 (Raport o kosztach naruszenia ochrony danych w 2024 r.), 30 lipca 2024 r.

5 marca 2025 2:11 / MKTG-185-0-0-EN