Praktyczny przewodnik dla kadry kierowniczej dotyczący zapobiegania utracie danych

Osiem etapów wdrożenia DLP na potrzeby ograniczenia ryzyka związanego z danymi i usprawnienia procesu zgodności z regulacjami

Forcepoint

Whitepaper

Spis treści

Nieskuteczność tradycyjnego podejścia do cyberbezpieczeństwa wobec współczesnych zagrożeń nie jest niespodzianką. Koncepcja środowiska pracy uległa całkowitej zmianie. Obecnie wymagany jest dostęp pracowników do najważniejszych z punktu widzenia działalności zasobów firmy z dowolnego miejsca.

Jak zachować kontrolę nad poufnymi danymi, gdy użytkownicy korzystają z niezabezpieczonych sieci Wi-Fi lub otwierają dokumenty na niezarządzanych urządzeniach osobistych? Co zrobić, aby uniemożliwić pracownikom udostępnianie zastrzeżonych lub chronionych informacji narzędziom AI na potrzeby trenowania dużych modeli językowych (LLM)? Jak zagwarantować ciągłą zgodność z coraz bardziej rygorystycznymi i licznymi przepisami dotyczącymi wykorzystania oraz prywatności danych?

Aby sprostać tym współczesnym wyzwaniom, konieczne jest zastosowanie rozwiązania z zakresu zapobiegania utracie danych (DLP Data Loss Prevention), które umożliwia zapobieganie udostępnianiu poufnych danych poza organizacją i blokowanie szeregu kanałów, którymi dane mogą zostać przekazane do osób nieupoważnionych.

Niniejszy przewodnik przedstawia proces wdrażania rozwiązania DLP, niezależnie od tego, czy przeprowadzasz go po raz pierwszy, zmieniasz dostawcę czy wykonujesz migrację usługi lokalnej do chmury. Koncentruje się na umieszczeniu rozwiązania DLP w centrum strategii bezpieczeństwa danych i osiąganiu wymiernych wyników, które umożliwiają ocenę powodzenia programu. Pozwoli to zapobiegać naruszeniom danych, usprawnić proces zgodności i kontrolować bezpieczeństwo we wszystkich kanałach komunikacji z pojedynczego punktu zarządzania.

Oto osiem etapów wdrożenia DLP, które przedstawimy:

1. Określenie celów i przypadków użycia
2. Opracowanie planu wdrożenia
3. Zdefiniowanie zasad DLP i procesów dotyczących incydentów
4. Wdrożenie DLP na potrzeby monitorowania
5. Przejście do aktywnego egzekwowania polityk
6. Ocena, udoskonalenie, zastosowanie
7. Rozszerzenie ochrony na inne kanały komunikacji
8. Rozbudowa polityk i fuknc jonalności

Podstawy strategii bezpieczeństwa danych

Aby zapewnić bezpieczeństwo danych organizacji, należy opracować odpowiedzi na pięć kluczowych pytań:

- → **Jakie** poufne dane mamy w ogranizacji?
- → **Gdzie** znajdują się poufne dane?
- → **Kto** może uzyskać dostęp do danych poufnych?
- → **W jaki sposób** dane poufne są wykorzystywane?
- → **Dlaczego** przyznawany jest dostęp do danych poufnych?

Strategia bezpieczeństwa danych powinna opierać się na zasadzie najniższego poziomu uprawnień (Principle of Least Privilege, POLP), zgodnie z którą użytkownicy powinni mieć dostęp tylko do informacji, które są niezbędne do wykonywania przydzielonych zadań. Do wdrożenia tej zasady niezbędne jest określenie typów wykorzystywanych danych oraz ich lokalizacji.

Stan danych w organizacji można opisać za pomocą jednego z następujących terminów. Są to:

- → **Dane w ruchu** (przesyłane w sieci)
- → **Dane w użyciu** (wykorzystywane w punkcie końcowym)
- → **Dane w spoczynku** (dane przechowywane w magazynie)
- → **Dane w chmurze** (w użyciu, w ruchu, w spoczynku)

Do zlokalizowania wymienionych typów danych i określenia ich typów niezbędna jest procedura odkrywania oraz klasyfikacji danych. Jeśli w organizacji jest już wykorzystywane co najmniej jedno rozwiązanie z tego zakresu, może stanowić solidną podstawę do zapobiegania utracie danych. Ten etap można również zrealizować po wdrożeniu rozwiązania DLP, gdy poufne dane są już chronione.

Zalecenia dostawców rozwiązań DLP dotyczące konieczności rozpoczęcia procesu od danych w spoczynku przed rozszerzeniem rozwiązania na pozostałe rodzaje danych nie są obowiązkowe. Solidna strategia bezpieczeństwa wymaga podjęcia szybkich działań w odpowiedzi na najpilniejsze wyzwania oraz opracowania planu działania na przyszłość. Punkt wyjścia dla wdrożenia powinien być określony na podstawie priorytetów organizacji. Niniejszy przewodnik przedstawia podejście polegające na wdrożeniu DLP w celu szybkiego przejścia do aktywnej ochrony, a następnie rozszerzeniu zakresu ochrony i dodaniu kolejnych funkcjonalności. Wykonanie wszytskich etapów ułatwi zapewnienie odpowiedniego stanu bezpieczeństwa danych z możliwością łatwego utrzymania oraz ciągłego ulepszania.

Przed rozpoczęciem wdrażania upewnij się, że wybrano najlepsze rozwiązanie DLP. Jeśli potrzebujesz pomocy przy wyborze dostawcy, zapoznaj się z naszym przewodnikiem po DLP dla kupujących.

Krok 1: Określenie celów i przypadków użycia

W pierwszej kolejności należy określić, czemu ma służyć wdrożenie DLP i jaki będzie główny obszar jego zastosowania. Dobrym początkiem jest opracowanie profilu ryzyka danych organizacji. Może to obejmować:

- → Wyszczególnienie potencjalnych konsekwencji braku działania
- → Opis rodzajów danych objętych zakresem (np. dane osobowe, własność intelektualna, dane finansowe)
- → Definicje sieci, punktów końcowych i kanałów chmurowych, w których dane mogą zostać utracone lub skradzione
- → Lista istniejących mechanizmów zabezpieczeń stosowanych obecnie na potrzeby ochrony danych (np. szyfrowanie)

Po określeniu wymienionych elementów można opracować listę najważniejszych przypadków użycia i celów wpływających na kluczowe cechy wdrożenia, co umożliwi opracowanie szczegółowego planu. Oto przykładowy schemat postępowania:

- → Określenie najważniejszych przypadków użycia
  - np. zabezpieczanie najważniejszych danych własności intelektualnej, zapobieganie naruszeniom danych, zgodność
- → Określenie celów krótkoterminowych i długoterminowych
  - Jakie cele biznesowe są powodem podjęcia działań?
    - Czy jest to określony termin zapewnienia zgodności z regulacjami?
    - Czy jest to zwiększenie skali pracy zdalnej lub hybrydowej?
  - Jakie są kluczowe daty w projekcie?
- → Określenie stanu bezpieczeństwa
  - Jaką pozycję zajmie DLP w istniejącej strukturze zabezpieczeń?
- → Identyfikacja najważniejszych kanałów
  - Gdzie należy rozpocząć wdrożenie?

Po zakończeniu tego etapu powinien być dostępny ogólny zarys wdrożenia i jego okresu. Następnie należy określić szczegóły wdrożenia.

Wizualizacja stosu technologii DLP
Identyfikacja nakładających się możliwości dotyczących różnych poziomów szczegółowości

PreciseID Fingerprinting
Dane strukturalne i niestrukturalne mogą być pobierane bezpośrednio z baz danych, dokumentów, arkuszy kalkulacyjnych itp. przy wysokiej skuteczności wykrywania nawet niewielkich podzbiorów danych opuszczających organizację

Klasyfikacja z wykorzystaniem sztucznej inteligencji
Stosuje chmurowy model AI trenowany z użyciem danych LLM oraz dostosowanej do określonej domeny generatywnej sztucznej inteligencji z uczeniem maszynowym

Skrypty NLP
Ponad 300 predefiniowanych opcji dostępnych w różnych językach. Inteligentne wykrywanie typów danych na podstawie opisanej zawartości z kontekstowymi pomocnikami zapewniającymi dokładność

Klasyfikacja i widoczność
Narzędzie obsługujące metadane (pliki, wiadomości e-mail itp.) umożliwiające przypisywanie etykiet oraz klasyfikację, które zapisuje znaczniki metadanych do plików

Typy plików
Ponad 900 typów plików wykrywanych na podstawie rzeczywistego rodzaju pliku w celu identyfikacji wszystkich typów plików bez względu na zmianę nazwy mającą uniemożliwić rozpoznanie

Wyrażenia regularne
Wyrażenia regularne oparte na języku Perl zapewniające kompleksowe, szczegółowe i dokładne wykrywanie treści

Frazy kluczowe
Ponad 1000 predefiniowanych słów kluczowych, fraz i wyrażeń słownikowych z zakresu przepisów i zgodności

Funkcje wybranego rozwiązania DLP mogą nie odpowiadać w pełni przedstawionym, ale będzie ono obejmować szereg technik, takich jak wykrywanie rzeczywistych typów plików, wyrażeń regularnych, skryptów NLP, tworzenie odcisków cyfrowych itd. do analizy danych. Podczas podejmowania wyboru określonego rozwiązania DLP należy porównać listy możliwości.

Ilustracja 1: możliwości DLP w zakresie wykrywania

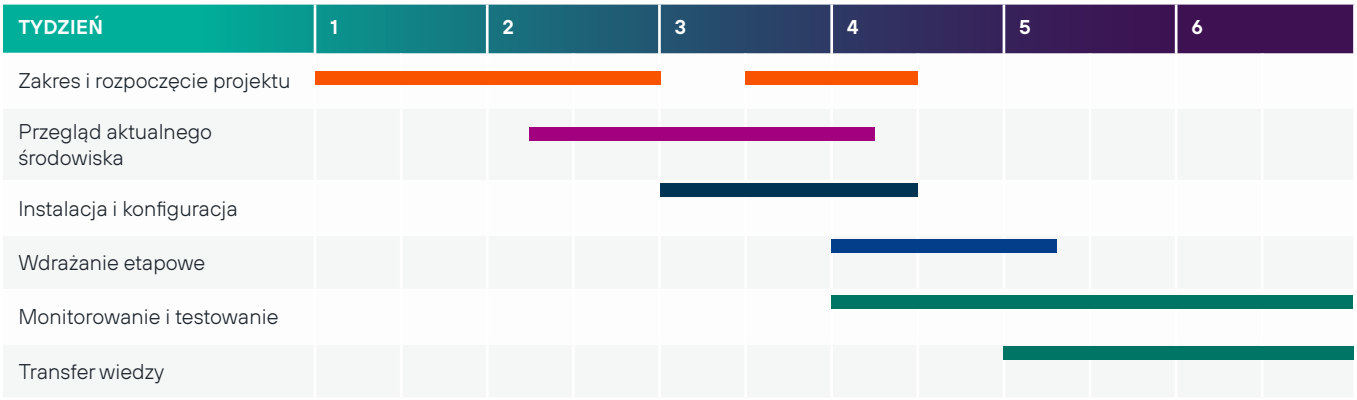
Etap 2: Opracowanie planu wdrożenia

Opracowanie planu wdrożenia rozpoczyna się od określenia ról poszczególnych zespołów w projekcie. Lista najważniejszych grup oraz i ich funkcji może wyglądać następująco:

ZESPÓŁ PODSTAWOWY	WYMAGANE UMIEJĘTNOŚCI
Kierownik projektu / Analitycy biznesowi / Specjaliści ds. ryzyka i zgodności	Gromadzenie wymagań, umiejętności dokumentacyjne, wiedza koncepcyjna na temat ochrony danych
Architekci / Starsi inżynierowie	Znajomość struktury sieci lokalnej i globalnej, przepływu danych oraz zarządzania operacyjnego
Sieć / Bezpieczeństwo / Inżynierowie systemów	Instalacja, konfiguracja i konserwacja rozwiązania oraz komponentów
Ekspert ds. bezpieczeństwa danych	Opracowanie reguł, przypadków użycia, identyfikacja elementów danych, dostosowanie zasad itp.
Badacze incydentów	Obowiązki dotyczące prywatności i ryzyka związane z dochodzeniami dotyczącymi wyprowadzania danych
Obsługa incydentów	Reagowanie na zdarzenia dotyczące bezpieczeństwa i alarmowanie
Eskalacja zdarzeń dotyczących bezpieczeństwa danych	Monitorowanie i bieżąca eskalacja

Ilustracja 2: najważniejsi członkowie zespołu oraz umiejętności niezbędne do realizacji planu wdrożenia

Po określeniu obowiązków można ustalić dopasowanie poszczególnych etapów planu wdrożenia do założonego okresu. Użyj przedstawionego formatu, aby jasno określić termin ukończenia zadań i regularnie korzystaj z harmonogramu projektu, aby upewnić się, że prace postępują zgodnie z założeniami. Przygotuj się do ponownego przeanalizowania harmonogramu, jeśli proces wdrażania zostanie zablokowany na dowolnym etapie.



Ilustracja 3:: harmonogram wdrożenia DLP

Harmonogram powinien opierać się na ocenie dostępnych zasobów i potrzeb projektu. Każde wdrożenie ma określone ramy czasowe, ale nasze rozwiązanie wspierało udane wdrożenia DLP jako SaaS w zaledwie sześć tygodni

Etap 3:
Zdefiniowanie zasad DLP i procesów dotyczących incydentów

Po ustaleniu podstaw zarządzania projektem wdrożenia należy ustalić, jakie zasady będzie egzekwować rozwiązanie DLP. Ustalenia te są oparte na określonym wpływie utraty, kradzieży lub naruszeniu poszczególnych rodzajów danych w organizacji.

Zacznij od prostego ćwiczenia z tablicą. Zorganizuj spotkanie zespołu wdrażającego DLP z właścicielami danych i partnerami, aby określić poziom wpływu utraty, kradzieży lub naruszenia danych. Można opisać wpływ za pomocą analizy jakościowej, takiej jak umieszczenie typów incydentów na skali od 1 do 5. Pomaga to ustalić priorytety działań dotyczących reagowania na incydenty i jest wykorzystywane do określenia odpowiedniego czasu reakcji.

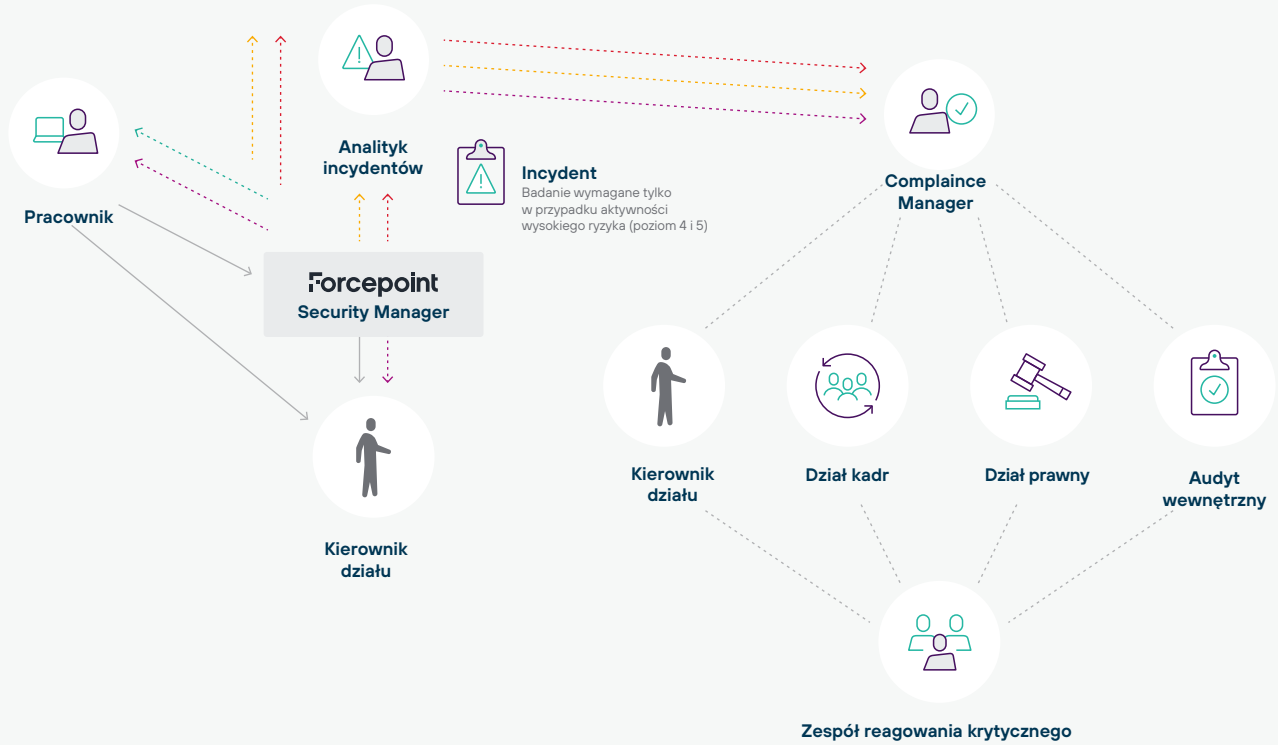
KANAŁY	POZIOM 1 NISKI	POZIOM 2 NISKI-ŚREDNI	POZIOM 3 ŚREDNI	POZIOM 4 ŚREDNI-WYSOKI	POZIOM5 WYSOKI	NOTES
Sieć	Audyt	Audyt / powiadomienie	Blokada / powiadomienie	Blokada / alert	Blokada	Proxy do zablokowania
Bezpieczna sieć	Audyt	Audyt / powiadomienie	Blokada / powiadomienie	Blokada / alert	Blokada	Inspekcja SSL
E-mail	Encrypt	Drop Email Attachments	Kwarantanna	Kwarantanna	Blokada	Szyfrowanie
FTP	Audyt	Audyt / powiadomienie	Blokada / powiadomienie	Blokada / alert	Blokada	Proxy do zablokowania
Drukarka sieciowa	Audyt	Audyt / powiadomienie	Blokada / powiadomienie	Blokada / alert	Blokada	Instalacja agenta drukarki DLP
Aplikacje chmurowe	Audyt	Audyt / powiadomienie	Kwarantanna z powiadomieniem	Kwarantanna	Blokada	Do ustalenia
Niestandardowe	Audyt	Audyt / powiadomienie	Blokada / powiadomienie	Blokada / alert	Blokada	Do ustalenia

Ilustracja 4: przykłady zasad DLP

Należy również opracować plan działań dotyczących incydentów, aby określić przebieg zdarzeń wywołanych określonym incydentem związanym z bezpieczeństwem. W przypadku incydentów o niskim stopniu zagrożenia należy stosować automatyzację, jeśli jest dostępna. Zwykle obejmuje to powiadamianie użytkowników i menedżerów o ryzykownych zachowaniach. Może również obejmować szkolenie pracowników w zakresie samodzielnego ograniczania skutków występującego zagrożenia. Incydenty o większym wpływie wymagają interwencji analityka, który zbada i określi rodzaj zagrożenia (np. przypadkowe, celowe lub złośliwe). Analityk incydentów przekazuje incydent i jego analizę menedżerowi programu – zwykle kierownikowi działu bezpieczeństwa lub zgodności – który następnie określa, jakie działania należy podjąć i jakie zespoły uwzględnić.

Proces oparty na wpływie i priorytecie incydentu

Rozwiązanie DLP dostosowujące się do ryzyka zapewnia egzekwowanie zasad na każdym poziomie ryzyka



Niski (poziom 1)	Audyt	Średni-wysoki (poziom 4)	Ograniczenie / badanie / automatyczne egzekwowanie zasad
Niski-średni (poziom 2)	Audyt i powiadomienie		
Średni (poziom 3)	Ograniczenie / powiadomienie / automatyczne egzekwowanie zasad	Wysoki (poziom 5)	Zatrzymanie / badanie / automatyczne egzekwowanie zasad

Ilustracja 5: proces dotyczący incydentu rozwiązania DLP

Po przygotowaniu powyższych można je wykorzystać jako podstawę do opracowania zasad DLP, które zostaną wprowadzone podczas następnej fazy: wdrażania.

Etap 4: Wdrożenie DLP na potrzeby monitorowania

Teraz następuje faktyczne wdrożenie rozwiązania z zakresu zapobiegania utracie danych. Przed aktywnym zastosowaniem DLP należy przeprowadzić wdrożenie pasywne umożliwiające poznanie konsekwencji określonych zasad w przypadku, gdy nieścisłości powodują nadmierne blokowanie aktywności, które nie wiążą się z zagrożeniem. Po uzyskaniu lepszego wglądu w przepływ danych oraz ich wykorzystywanie w organizacji można zmodyfikować mechanizmy kontroli, aby egzekwować stosowanie zasad wobec użytkowników lub incydentów wyższego ryzyka.

Wdrożenie rozwiązania DLP nie powinno sprawiać trudności pod warunkiem odpowiedniego zaplanowania i poinformowania odpowiednich grup użytkowników. Typowe wdrożenie powinno przebiegać zgodnie z przedstawionym procesem, który można wykorzystać do potwierdzenia, że nie pominięto żadnych ważnych kroków.

Instalacja

- → Skorzystaj ze wsparcia technicznego dostawcy, aby pomyślnie przeprowadzić wdrożenie
- → Przed wdrożeniem przeprowadź testy na wybranych użytkownikach.

Konfiguracja

- → Określenie zasad, procesów i wskaźników
- → Test przeciążeniowy wykorzystujący próbki danych z ruchu klientów na żywo
- → Określanie priorytetów i eliminowanie luk przy użyciu znanych rozwiązań
- → Testowanie akceptacyjne przez użytkowników (UAT)

Etapowe ograniczanie ruchu produkcyjnego

- → Przeprowadzenie po godzinach
- → Wdrożenie według kanału lub regionu
- → Monitorowanie przez kolejny tydzień w celu potwierdzenia prawidłowego działania środowiska na żywo

Dostosowanie i udoskonalenie

- → Ograniczenie przypadkowych incydentów poprzez dodanie wyjątków lub wyłączeń
- → Tworzenie różnych poziomów zasad i niestandardowych raportów dostosowanych do potrzeb przypadków użycia
- → Tworzenie powiadomień i alertów dotyczących incydentów oraz kondycji systemu

Ten proces obejmuje wdrożenie mechanizmów kontroli sieci DLP, przeprowadzenie analizy i przedstawienie najważniejszych wniosków kadrze kierowniczej. Powinny one obejmować zalecenia dotyczące działań ograniczających częstotliwość występowania zagrożeń danych. Następnie należy zebrać wyniki i przedstawić je kadrze kierowniczej.

Najlepszym podejściem jest wdrażanie etapami, chociaż można zastosować inną strukturę wdrożenia. Można rozpocząć od określonego kanału (np. punktu końcowego) lub przyjąć podejście organizacyjnie (według działu) albo geograficzne (według kraju lub regionu w większych krajach). Możliwe jest również zastosowanie połączenia wymienionych podejść. Działanie według regionu umożliwia wykorzystanie przedziałów czasowych poza godzinami pracy na każdym etapie wdrażania, aby ograniczyć zakłócenia działalności.

Na tym etapie rola mechanizmów kontroli DLP polega przede wszystkim na monitorowaniu i blokowaniu wyłącznie poważnych incydentów (np. przesyłania danych do znanych złośliwych miejsc docelowych lub masowego przesyłania niezabezpieczonych rekordów zagrożonych w ramach pojedynczej transakcji).

Etap 5:
Przejście do aktywnego egzekwowania polityk

Po zakończeniu dostosowania zasad DLP i dodawania wyjątków w zależności od potrzeb można przejść do aktywnego blokowania zagrożeń.

Zacznij od stopniowego wdrażania aktywnego blokowania. Należy nadać priorytety najbardziej krytycznym transferom danych i stopniowo rozszerzać je na inne obszary, aby zminimalizować wpływ na działalność biznesową.

Nieustannie monitoruj skuteczność aktywnego blokowania. Przeglądaj zablokowane incydenty i dostosuj zasady w razie potrzeby, aby zapobiec blokowaniu działań niezwiązanych z ryzykiem.

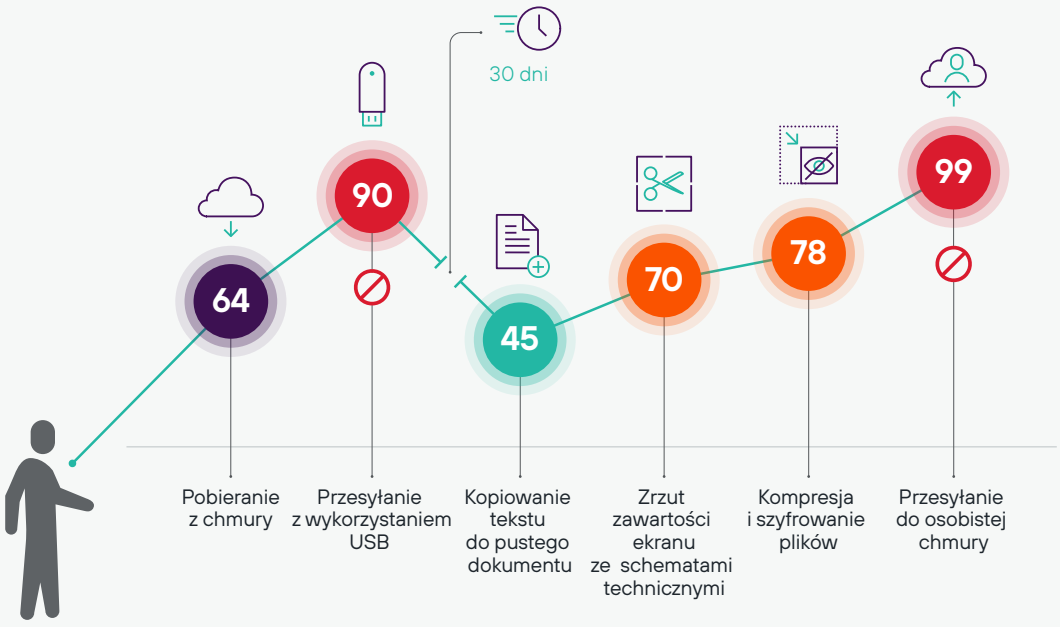
Po wprowadzeniu skutecznego aktywnego blokowania działań naruszających zasady DLP należy skonfigurować mechanizmy automatyzacji, które skrócą czas reakcji i jednocześnie zmniejszą obciążenie administratorów związane z analizowaniem incydentów. Wybrane rozwiązanie z zakresu DLP powinno umożliwiać automatyzację egzekwowania zasad, ale można również wykorzystać możliwość dynamicznego dostosowania egzekwowania do zachowań użytkowników.

Rozwiązanie takie jak Forcepoint Risk-Adaptive Protection umożliwia zastosowanie w pełni zautomatyzowanego podejścia, zapewniając ocenę ryzyka zachowań użytkowników i dostosowując zabezpieczenia do indywidualnych potrzeb na podstawie tej oceny, która jest prowadzona dynamicznie z wykorzystaniem zachowania poszczególnych użytkowników w czasie. Ścisła integracja z rozwiązaniem DLP Forcepoint umożliwia dostosowywanie uprawnień do oceny ryzyka, ograniczając liczbę wyników fałszywie dodatnich i zapewniając alerty na podstawie priorytetu. System klasyfikacji oszczędza czas administratorów, umożliwiając im przeciwdziałanie rzeczywistym zagrożeniom, co zapewnia optymalną pracę użytkowników.

Działania o niskim stopniu ryzyka są dozwolone, natomiast działania o wyższym stopniu ryzyka generują automatyczne reakcje, które obejmują różne obszary – od ostrzeżeń dla administratorów lub użytkowników końcowych i rekomendacji po szyfrowanie i całkowite blokowanie. Zapewnia to maksymalne ograniczenie zakłóceń działalności organizacji, wstrzymując niebezpieczną aktywność bez nadmiernego blokowania zwykłych użytkowników i systemów.

Ustalanie dynamicznych ocen ryzyka

Sposób przypisania przez system oceny ryzyka od 0 do 100 na podstawie różnych działań użytkownika



Ilustracja 6: przykładowe oceny ryzyka aktywności w różnych kanałach

Etap 6: Ocena, udoskonalenie, powtórzenie

Po zakończeniu wdrożenia należy przeprowadzić ilościowe określenie wpływu rozwiązania DLP na działalność biznesową, aby zmierzyć zwrot z inwestycji. Można uzyskać odpowiednie dane ze śledzenia incydentów i utworzyć raporty pokazujące, w jakim stopniu ryzyko zostało ograniczone po wdrożeniu i przejściu na aktywne blokowanie. Oto kilka wskazówek umożliwiających uzyskanie dokładnych wyników umożliwiających działanie:

- **Grupowanie powiązanych incydentów.** Przykładowe grupy można utworzyć w oparciu o wpływ, kanał, typ danych i przepisy. W przypadku większych organizacji dodatkowe podgrupy pomagają lepiej określić ryzyko według lokalizacji geograficznych lub jednostek zależnych.
- **Zachowanie spójności etapów ograniczania redukcji ryzyka.** Na potrzeby zachowania integralności wyników, okresy monitorowania i ograniczania ryzyka muszą mieć jednakową długość. Na początku zalecane są dwa tygodnie w celu skrócenia czasu do osiągnięcia korzyści oraz uproszczenia analizy. Należy jednak dostosować ten okres do potrzeb organizacji.
- **Oddzielenie reakcji automatycznych od reakcji ludzkich.** W przypadku wykorzystania ochrony dostosowanej do ryzyka należy przedstawić porównanie incydentów zarejestrowanych w trybie audytu (wszystkie incydenty) z incydentami wymagającymi badania i stopniowego egzekwowania. Podsumowanie powinno wskazywać liczbę incydentów dla każdego poziomu ryzyka 1–5 w zestawieniu z przypadkami, które faktycznie wymagają zbadania (poziomy ryzyka 4–5).

Zaplanowanie okresowych przeglądów w przyszłości z kontynuacją analizy danych w celu utrzymania niskiego poziomu ryzyka i dostosowania zasad DLP w przypadku wykrycia luki.

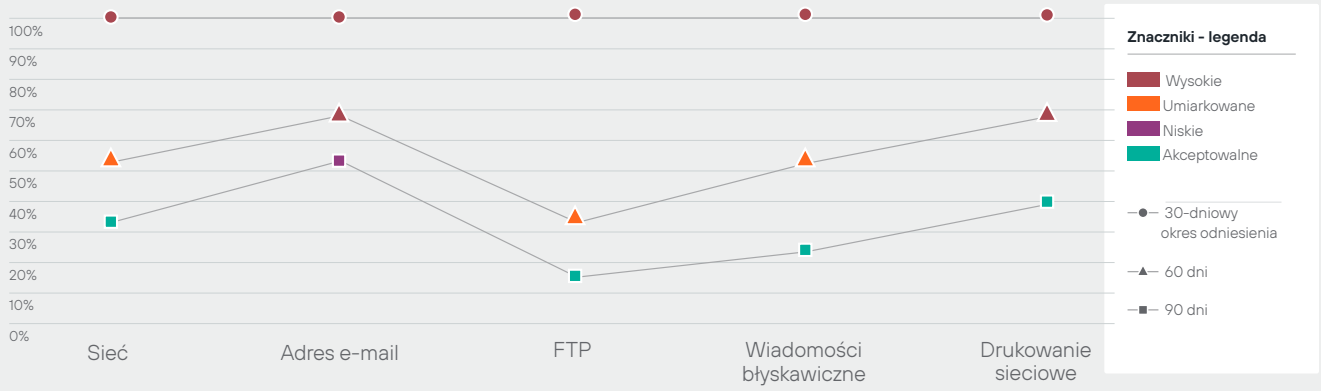
Do kluczowych elementów bieżących działań DLP należy szkolenie pracowników. Szkolenie pracowników można przeprowadzić na wiele sposobów, jednak zalecane są takie opcje jak:

- Organizacja ćwiczeń symulacyjnych przedstawiających poziomy ryzyka i możliwości jego ograniczenia
- Zapewnienie szkoleń dla zespołu administracyjnego i zespołu operacyjnego
- Tworzenie odpowiednich internetowych baz wiedzy (KB)
- Prowadzenie działań zwiększających świadomość zagrożeń i szkoleń produktowych dla zainteresowanych stron

Warunkiem prawidłowego wdrożenia jest iteracyjne podejście do zabezpieczeń z nieustannymi działaniami na rzecz poprawy i udoskonalenia istniejących procesów. Niezależnie od stanu zabezpieczeń zawsze dostępne są możliwości udoskonalenia.

Ograniczenie prawdopodobieństwa utraty danych z upływem czasu

Wyznaczenie celów i pomiar skuteczności ograniczenia ryzyka w określonych kanałach przez 60 dni, 90 dni i w dłuższym okresie

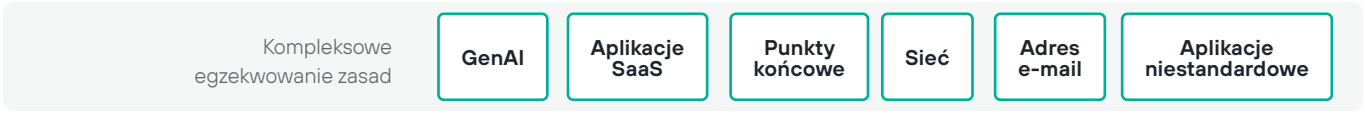


Ilustracja 7: śledzenie incydentów na potrzeby pomiaru ograniczenia ryzyka

Krok 7: Rozszerzenie ochrony na inne kanały

Zakończ proces wdrażania rozwiązania z zakresu DLP w organizacji, rozszerzając ochronę na pozostałe typy danych (np. dane w użyciu i dane w spoczynku) oraz kanały (np. Internet, poczta elektroniczna, aplikacje SaaS w chmurze i punkty końcowe). Być może na początku wprowadzono ochronę kilku najważniejszych aplikacji w chmurze, a teraz należy rozszerzyć ochronę na pozostałe.

Bez względu na sytuację początkową wymagana jest możliwość wykorzystania istniejących zasad DLP z jednego kanału do egzekwowania we wszystkich pozostałych kanałach. Ta funkcja jest niezbędna do szybkiego wdrożenia kompleksowej ochrony wszystkich sposobów przesyłania danych w organizacji. Możesz powielać istniejące zasady w celu szybkiego działania, a następnie dostosować je w przypadku różnych wymagań poszczególnych kanałów w tym zakresie.



Ilustracja 8: egzekwowanie zasad DLP w wielu kanałach

Rozszerzenie ochrony można wygodnie zrealizować poprzez zastosowanie odpowiednich narzędzi dla poszczególnych kanałów, takich jak CASB i SWG. Możliwe jest również zapewnienie bezpieczeństwa transferów realizowanych za pośrednictwem poczty e-mail.

Główna część wdrożenia zostanie zakończona, gdy system DLP aktywnie i automatycznie egzekwuje zasady we wszystkich kanałach danych. Należy przygotować się na dalszą optymalizację zasad w przyszłości wraz z wprowadzaniem w organizacji większej liczby aplikacji, fizycznych lokalizacji, typów danych itp. Rozważ dodatkowe możliwości, które zwiększą skuteczność i dokładność programu ochrony danych, jednocześnie ograniczając narażenie na zagrożenia związane z danymi.

Etap 8:
Dodanie rozszerzonych możliwości

Usprawnienie procesów odkrywania i klasyfikacji danych stanowi solidną podstawę dla bieżących działań w zakresie DLP. Wyraźne określenie typów poufnych danych oraz ich lokalizacji gwarantuje egzekwowanie odpowiednich zasad przez cały cykl życia danych.

Najlepszym sposobem wdrożenia tego proaktywnego podejścia jest wykorzystanie możliwości rozwiązania z zakresu zarządzania stanem bezpieczeństwa danych (DSPM – Data Security Posture Managment). Może to znacznie zwiększyć skuteczność rozwiązania DLP poprzez dokładne wykrywanie i klasyfikowanie danych, co prowadzi do ograniczenia liczby wyników fałszywie dodatnich, umożliwiając administratorom koncentrację działań na usuwaniu incydentów, audytach i aranżacji procesów. Rozwiązanie DSPM ogranicza ryzyko związane z danymi poprzez minimalizację danych ROT („nadmiarowe, nieistotne, przestarzałe") i zapewnienie kontroli nad nimi. Tego typu rozwiązanie umożliwia identyfikację przypadków nadmiernych uprawnień dotyczących plików (np. dokumenty poufne dostępne publicznie) w celu egzekwowania zasady najniższego poziomu uprawnień (PoLP).

Rozwiązanie DSPM powinno umożliwiać tworzenie raportów potwierdzających zgodność z przepisami regionalnymi i branżowymi, co przyspiesza proces audytu. Może również zapewniać scentralizowany widok danych dostępnych w chmurze oraz w lokalizacjach sieciowych, co ułatwia wdrażanie i egzekwowanie zasad zarządzania danymi.

Wdrożenie rozwiązania DSPM zapewnia solidną podstawę dla działań DLP, proaktywnie tworząc środowisko, w którym DLP może przynieść największe korzyści przy ograniczonej do minimum konieczności działania administratorów. Warunkiem skuteczności DLP jest określenie dostępnych danych. Im lepsza klasyfikacja danych i ogólny stan bezpieczeństwa danych, tym skuteczniejsze jest rozwiązanie DLP.

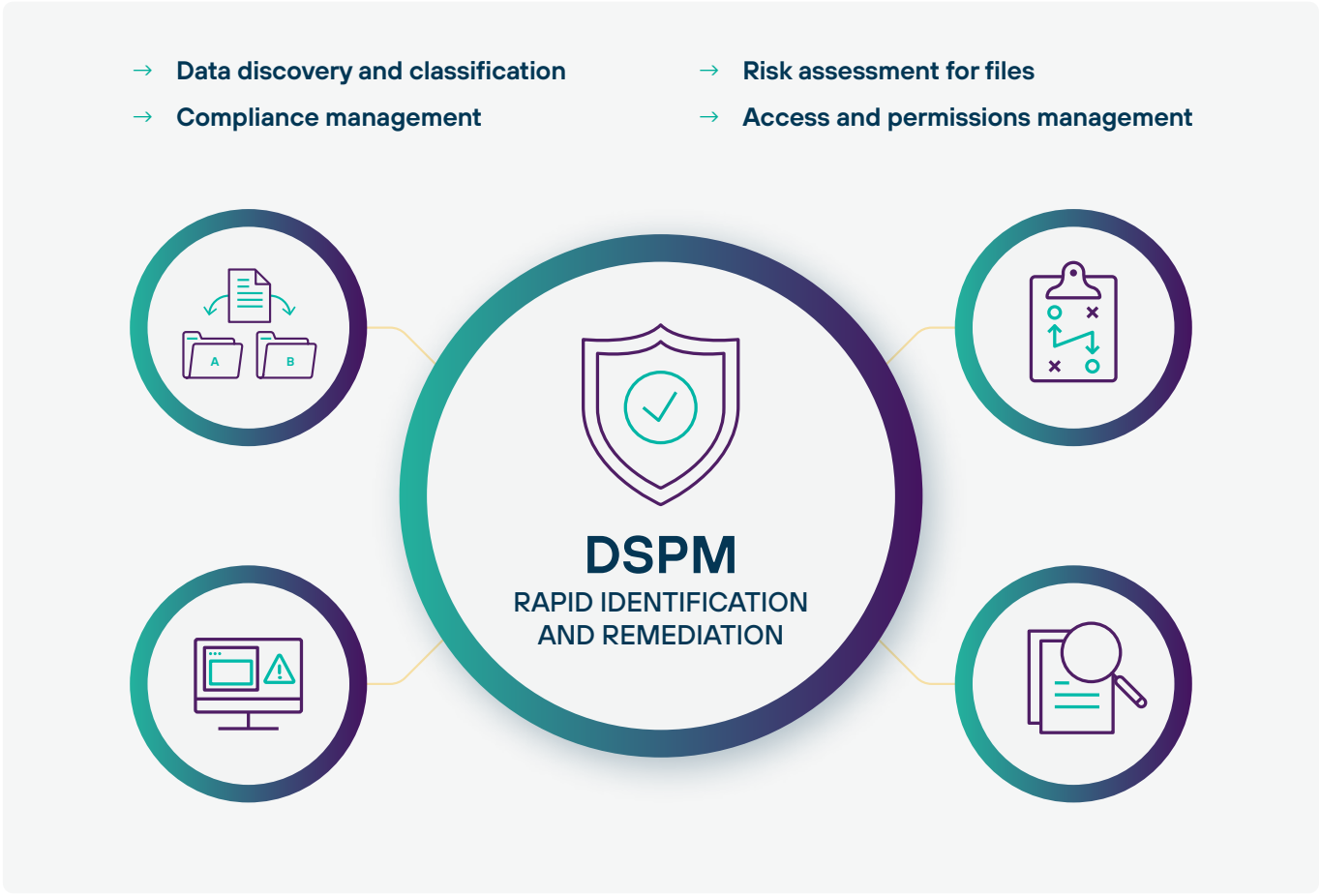
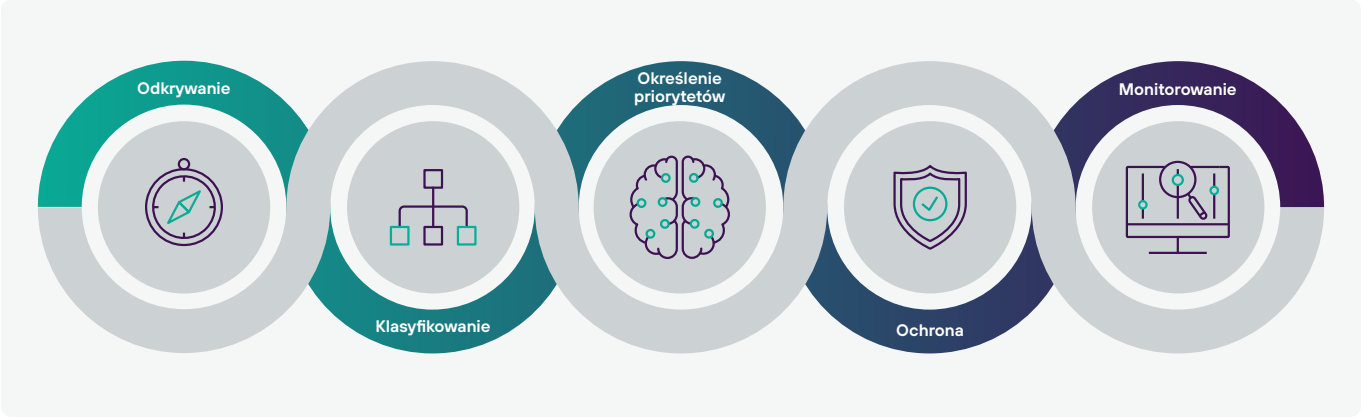


Figure 9: The core functionalities of DSPM

Wniosek:
Ochrona przez cały cykl życia danych

Zagrożenie dla danych to ryzyko dla firmy. Podejście oparte na cyklu życia danych minimalizuje ryzyko w obu obszarach. Wymaga to nieustannej analizy wszystkich etapów przetwarzania danych oraz łączenia procesów proaktywnych i reaktywnych w celu zapewnienia kompleksowej ochrony, ujednoliconej widoczności i kontroli. Takie podejście nazywamy kompleksowym bezpieczeństwem danych (Data Security Everywhere).



Ilustracja 10: przedstawienie etapów podejścia kompleksowego bezpieczeństwa danych

Najważniejsze zasady kompleksowego bezpieczeństwa danych:

- **Odkrywanie** lokalizacji poufnych danych za pomocą szybkiego skanowania w całej organizacji na potrzeby identyfikacji nadmiarowości danych oraz innych zagrożeń
- **Klasyfikacja** danych z jak największą dokładnością, aby zapewnić spójność zasad i raportowania oraz zapewnić maksymalną skuteczność blokowania naruszeń bezpieczeństwa danych przez rozwiązanie DLP
- **Określenie priorytetów** działań na rzecz bezpieczeństwa danych z wykorzystaniem możliwości rozszerzenia ochrony na dodatkowe kanały lub aplikacje
- **Ochrona** własności intelektualnej i danych podlegających regulacjom prawnym w całej organizacji poprzez zapobieganie wyprowadzaniu danych oraz zapewnienie zgodności z przepisami
- **Monitorowanie** ryzyka związanego z danymi na potrzeby dynamicznego dostosowania zasad, przeciwdziałania zagrożeniom wewnętrznym i ograniczania czasochłonnych wyników fałszywie dodatnich

Połączenie rozwiązania DLP (rozszerzonego o ochronę dostosowaną do ryzyka) i DSPM stanowi podstawę ciągłej strategii na rzecz ograniczenia ryzyka związanego z danymi w całej organizacji, zapewniając solidną podstawę kompleksowego systemu bezpieczeństwa danych bez względu na lokalizację dostępu użytkowników oraz urządzeń do sieci.

Mamy nadzieję, że niniejszy przewodnik okaże się pomocny podczas planowania i realizacji wdrożenia DLP. Na stronie forcepoint.com można znaleźć więcej infroacji dotyczących DLP lub zamówić wersję próbną wybranego rozwiązania z naszej oferty

Forcepoint

forcepoint.com/contact

Informacje o Forcepoint

Misją Forcepoint jest ułatwienie procesu zapewnienia bezpieczeństwa na potrzeby firm i organizacji rządowych na całym świecie. Działająca całkowicie w chmurze kompleksowa platforma Forcepoint ułatwia wdrożenie modelu Zero Trust oraz zapobieganie kradzieży lub utracie danych poufnych i własności intelektualnej bez względu na charakter i lokalizację wykonywanej pracy. Forcepoint z siedzibą w Austin w stanie Teksas tworzy bezpieczne i zaufane środowiska dla klientów oraz pracowników w ponad 150 krajach. Skontaktuj się z Forcepoint na stronie forcepoint.com, w serwisie X oraz LinkedIn.

[Practical-Exec-Guide-to-DLP-Whitepaper-PL] 31Jan2025