FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP

AALEXANDER RACZYNSKI

Forcepoint DLP

Forcepoint DLP jest rozwiązaniem DLP oferowanym przez firmę Forcepoint. Rozwiązanie to jest interesujące nie tylko ze względu na potwierdzoną jakość produktu, ale również ze względu na to, że Firma Forcepoint posiada w Polsce referencje w postaci klientów również w sektorze finansowo-ubezpieczeniowym i innych.

W skład pakietu Forcepoint DLP wchodzą zarówno komponenty DLP sieciowego (DLP Network), jak i DLP hostowego (DLP Endpoint) wykorzystujące wspólny model zasad, które dają wgląd i kontrolują ochronę danych w sieci i punktach końcowych, a także zapewniają kompleksowe wykrywanie danych w korporacyjnych systemach przechowywania danych (DLP Discover).

Jadnak nie tylko walory technologiczne decydują o tym, że Forcepoint DLP jest rozwiązaniem chętnie wybieranym przez klientów. Produkt został zaprojektowany tak, by maksymalnie ułatwić implementację rozwiązania w organizacji. Słowo „implementacja" obejmuje w tym wypadku nie tylko sam proces instalacji systemu. Dużo ważniejsze są bowiem procesy biznesowe i administracyjne, które z projektem DLP są nierozłącznie związane.

System Forcepoint DLP został zaprojektowany tak, by maksymalnie ułatwić wdrożenie, początkową implementację polityk i zminimalizować nakłady związane z administrowaniem incydentów DLP.

Poniżej opisano niektóre funkcjonalności, które umożliwiają te zadania.

Technologie DLP

Systemy DLP wdraża się w organizacjach przetwarzających informacje niejawne, których ujawnienie może narazić organizację na odpowiedzialność karną lub cywilną. Wdrożenia DLP służą najczęściej realizacji prawnych lub branżowych wymogów ochrony danych osobowych i finansowych.

Systemy DLP mogą wykorzystywać wiele technik do kontroli przepływu informacji niejawnych:

- wykrywanie danych wrażliwych w ruchu sieciowym w sposób podobny jak systemy wykrywania włamań lub w plikach zapisywanych na nośniki zewnętrzne w sposób podobny do programów antywirusowych,
- klasyfikacja i przypisanie wag plikom w lokalnym systemie na podstawie zawartości danych wrażliwych, a następnie kontrolowanie przesyłania tych plików przez sieć lub zapisywania ich na nośniki zewnętrzne,
- blokowanie zapisu na nośniki zewnętrzne w ogóle,
- transparentne szyfrowanie i deszyfrowanie wrażliwych dokumentów tak, by nigdy nie opuszczały one organizacji w formie niezaszyfrowanej, zaś wewnątrz niej były czytelne tylko dla osób uprawnionych (systemy zarządzania prawami do informacji – IRM).

Podstawowe technologie DLP

Rozwiązania technologiczne, zapobiegające przeciekom danych, opierają się na dwóch podstawowych koncepcjach architektonicznych :sieciowej i działającej w punkcie końcowym (opartej na agentach).Obie mają swoje wady i zalety. Rozwiązanie sieciowe obejmuje swoim zasięgiem wszystkie punkty końcowe w sieci, niezależnie od systemu operacyjnego czy też funkcji określonego komputera. Zaletą takiego rozwiązania jest stosunkowo łatwe wdrożenie, w porównaniu do wdrażania poszczególnych agentów na wszystkich chronionych komputerach. Jeśli jednak rozwiązanie sieciowe ma blokować podejrzany ruch w sieci, to musi być umieszczone w strumieniu danych lub współdziałać z urządzeniem sieciowym, przez które przechodzi ten strumień. Rozwiązania oparte na agentach mają większy zasięg. Agent zainstalowany w punkcie końcowym może wykryć i zablokować transfer poufnych informacji do urządzeń podłączonych lokalnie, który nie zostałby wykryty przez rozwiązanie sieciowe. Rozwiązania instalowane w punkcie mogą również zapewnić ochronę urządzenia, gdy nie jest ono połączone do sieci w firmie

(na przykład wtedy, gdy służbowy laptop jest używany w domu i podłączony do obcej sieci, do Internetu).

Sieciowe DLP

Koncepcja sieciowego DLP (DLP Network) zakłada instalację systemu filtrującego dane na styku z Internetem lub na brzegu chronionej podsieci. System – najczęściej dedykowane urządzenie – skanuje wychodzący ruch pod kątem nieautoryzowanych transmisji danych. Zaletą tej techniki jest stosunkowo proste wdrożenie: brak konieczności instalowania agenta na chronionych stacjach roboczych. Ponieważ analiza danych transmitowanych przez sieć w czasie rzeczywistym przy coraz większych prędkościach transmisji nie jest rzeczą łatwą, tego typu rozwiązania umożliwiają analizę danych na wskazanych serwerach. Analiza taka polega na przesłaniu dokumentów z chronionego repozytorium na urządzenie DLP, gdzie są one sprawdzane i wykonywany jest ich skrót cyfrowy (fingerprint) w trybie offline. Popularną techniką wykonywania skrótu danych, wykorzystywaną w tego typu rozwiązaniach jest Sliding Window. Pozwala ona na tworzenie dokładnych sygnatur dokumentów. Urządzenie skanujące przechowuje sygnatury dokumentów i wykorzystuje je do analizy ruchu sieciowego wychodzącego z chronionego segmentu. Problemem jest tu wielkość sygnatury, która rośnie proporcjonalnie do wielkości dokumentu. Standardowe sieciowe DLP nie radzą sobie z analizą danych, przesyłanych za pomocą szyfrowanych protokołów, takich jak HTTPS czy też z prywatnych kont pocztowych pracowników lub komunikatorów internetowych. Nie poradzą sobie również z transferem danych z komputerów pracowników na pamięci wymienne czy zrzutami ekranowymi, wysyłanymi zamiast dokumentów.

Hostowy DLP

Do ochrony przed wyciekiem danych przez prywatne konta poczty elektronicznej pracowników, porty USB, korporacyjną pocztę czy aplikacje w rodzaju Google Docs wewnątrz połączenia SSL, konieczne jest rozwiązanie działające na komputerach użytkowników – DLP hostowe (Endpoint/Agent Based DLP). W odróżnieniu od rozwiązań sieciowych, opiera się ono na agentach działających na stacjach roboczych i serwerach. Ich zadaniem jest monitorowanie wszystkiego, co dzieje się z chronionymi informacjami, niezależnie od tego, gdzie operacje na danych mają miejsce. Hostowe DLP, tak jak rozwiązania sieciowe, korzystają z technik analizy skrótów danych, mogą więc określać, czy sprawdzany tekst powinien być chroniony, czy też nie. Sygnatury danych są przechowywane na stacjach roboczych, gdzie następuje weryfikacja zdarzeń, pod kątem ich zgodności z przyjętymi regułami polityki. Wykorzystywane są także filtry słów kluczowych oraz metadanych. Dla słów kluczowych można ustawić filtry tak, żeby z każdym wyrazem z ustalonej listy, pojawiającym się w sprawdzanym dokumencie, zwiększała się punktacja ryzyka. Natomiast wykorzystując metadane, można blokować pliki o danych właściwościach, co nie musi mieć wyraźnego związku z ich treścią. Za pomocą hostowego DLP można kontrolować nieautoryzowane zapisy poufnych danych na nośniki CD/DVD czy USB, a także ich drukowanie. Można też uniemożliwić tworzenie zrzutów ekranowych i przekazywanie ich na zewnątrz w postaci plików graficznych. Przy tym należy podkreślić, że bardzo wielką rolę gra nie tylko samo blokowanie akcji, ale edukacja użytkowników. Czasami bardzo skuteczne jest samo poinformowanie użytkownika o tym, że dana akcja może być naruszeniem polityki bezpieczeństwa obowiązującej w organizacji i może nieść za sobą poważne konsekwencje. Produkty DLP tego typu wykorzystują mechanizmy aktywnego ukrywania istnienia agenta, przy czym ukrywany jest nie tylko proces, ale czasami także pliki na dysku. Dzięki odpowiednio ustawionym uprawnieniom, nie jest możliwe wyłączenie agenta.

Podsumowując: sieciowe i hostowe DLP uzupełniają sie wzajemnie i razem dają najlepsze efekty. Istnieją producenci którzy oferują kompleksowe rozwiązanie DLP zarówno sieciowe jak i hostowe które pełnią funkcję zintegrowanego spójnego systemu ochrony przed wyciekiem danych.

Tego typu systemy oferują największe możliwości oraz integrują w sobie zalety systemów sieciowych jak i hostowych. Firmą oferującą tego typu rozwiązania jest firma Forcepoint, która

oprócz pełnego i kompleksowego systemu DLP oferuję także najlepsze w swojej klasie systemy ochrony ruchu WWW w tym ochronę Web 2.0. Integracja obydwu systemów – ochrony Web oraz Systemu DLP daje dodatkowe możliwości które nie oferuje obecnie żaden inny producent rozwiązań bezpieczeństwa na rynku.

Zalety rozwiązania Forcepoint DLP

Skalowalność systemu

System Forcepoint DLP jest systemem modułowym, który daje się skalować na potrzeby dużej organizacji Enterprise.

Triton Server

Sercem systemu jest moduł zarządzający Triton Server. Jest to oprogramowanie, które instaluje się na platformie Windows Server 2008 R2 lub 2012 (również wirtualnie). Triton Server jest platformą zarządzającą rozwiązaniami Forcepoint, która wykorzystuje się do definiowania polityk oraz zarządzania incydentami. Obsługa modułu zarządzającego odbywa się poprzez Web-GUI - Forcepoint Triton Manager

DLP Server

Niektóre zadania systemu mogą być przekazane do pomocniczego serwera DLP (DLP Server). Taki pomocniczy server jest również instalowany na platformie Windows Server 2008 R2 lub 2012 (również jako serwer wirtualny). Typowymi zadaniami, które są realizowane przez dodatkowy Server DLP jest fingerprinting informacji, analiza OCR. Często Server DLP jest wykorzystywany również jako serwer obsługujący Endpointy. W przypadku dużej organizacji takie postępowanie ma niewątpliwe tę zaletę, że Endpointy nie kontaktują się bezpośrednio z maszyną zarządzającą.

DLP Server nie jest wymogiem, a jedynie opcją skalowania systemu. Tworzenie dodatkowych serwerów DLP nie jest licencjonowane oddzielnie. W ramach licencji DLP można stworzyć dowolną ilość dodatkowych Serwerów DLP.

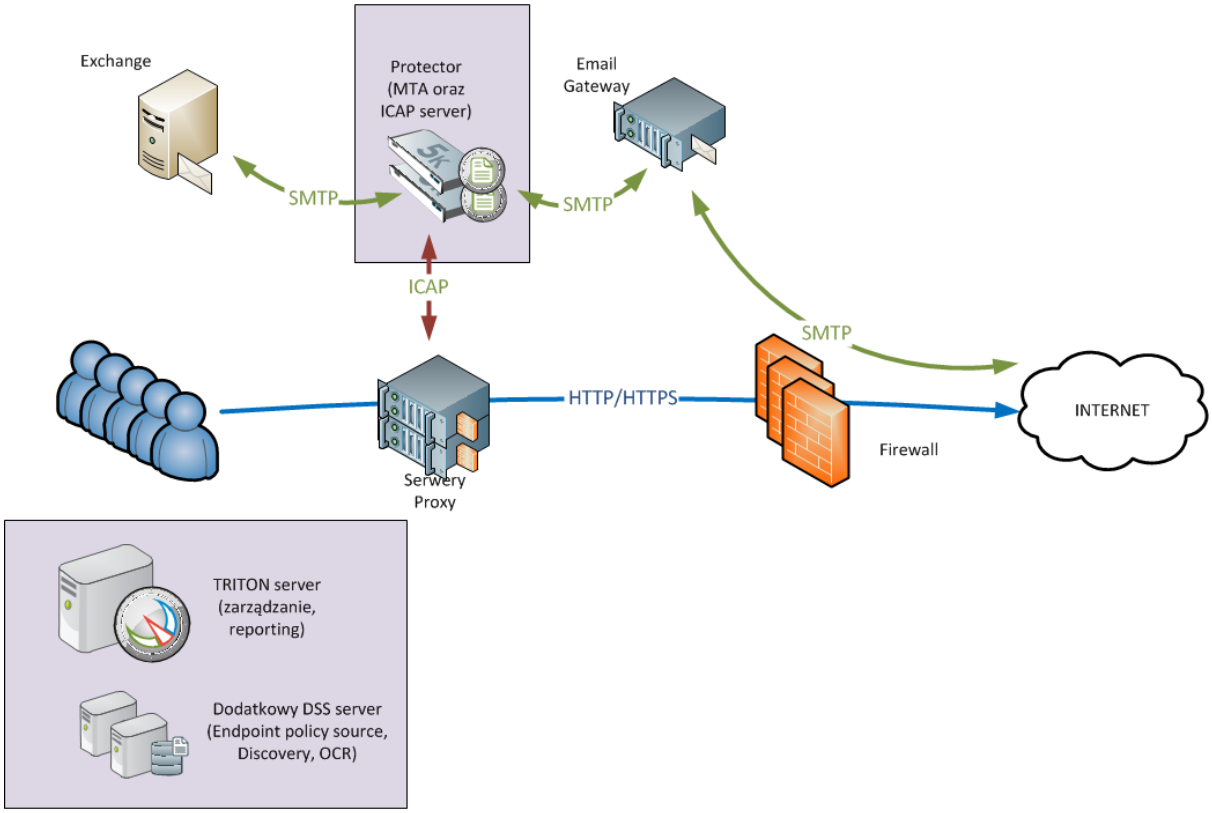
DLP Protector

Jest modułem instalowanym na dowolnej platformie sprzętowej (również wirtualnie). Jest to software appliance oparty o system Linux i dostarczany w ramach licencji DLP. Protector może pełnić różne funkcje w ramach sieciowego DLP. Jego typowymi zastosowaniami jest:

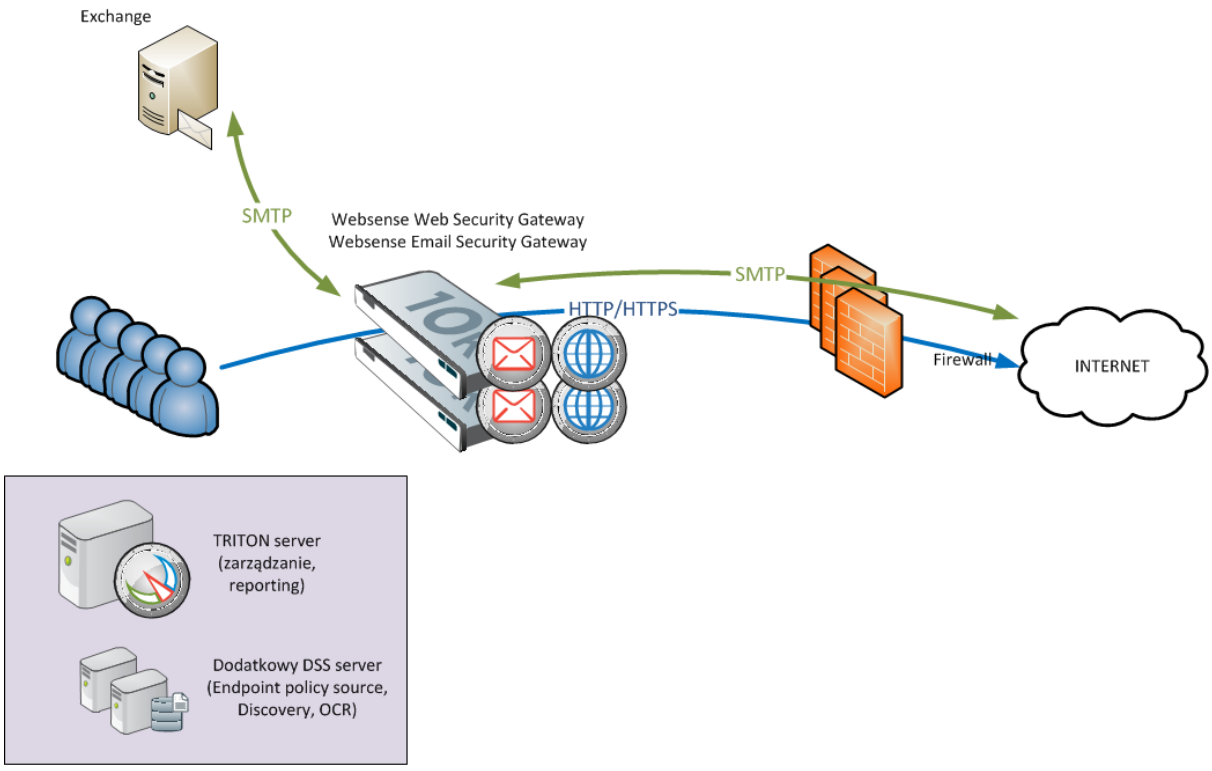
- praca w trybie MTA a celu analizy wychodzącej poczty elektronicznej
- ICAP server w celu integracji z istniejącym proxy firm trzecich
- praca w trybie proxy dla połączeń ActiveSync

Protector może być instalowany w dowolnych ilościach w ramach licencji DLP.

Szczegóły implementacji systemu zależą od istniejącej już infrastruktury sieciowej. W wielu przypadkach opierają się one o schemat załączony na poniższym rysunku.



Istnieje również możliwość integracji rozwiązania Forcepoint DLP z innymi rozwiązaniami firmy Forcepoint. Przykład implementacji rozwiązań w ramach jednego producenta jest przestawiony poniżej:



Integracja z istniejącymi rozwiązaniami

- WEB
  Dzięki możliwości zastosowania modułów typu Protector Forcepoint DLP integruje się bezproblemowo w

większością systemów typu proxy oferowanych na rynku. Jedynym wymaganiem stawianym rozwiązaniom typu proxy jest wsparcie dla protokołu ICAP. Należy tutaj wspomniec o fakcie, że w przypadku integracji z rozwiązaniem typu proxy, to od proxy zależy czy monitorowaniu zostanie poddany również ruch HTTPS. Jeżeli istniejące proxy ma moźliwości rozszywania ruchu SSL, to monitorowanie DLP jest również możliwe dla ruchu HTTPS.

- EMAIL
  Protector działający w trybie MTA jest łatwą i efektywną możliwością integracji z każdym serwerem email. Integracja polega tutaj na konfiguracji „next hop" dla serwera email i wskazanie urządzenia typu Protector.
- SIEM
  Forcepoint DLP integruje się bezproblemowo również ze wszystkimi znanymi rozwiązaniami typu SIEM. Protokół syslog umożliwia generowanie zdarzeń w samego systemu jak również zdarzeń mających związaek z generowaniem incydentów DLP.

Licencjonowanie systemu Forcepoint DLP

Licencjonowanie systemu DLP jest oparte o liczbę chronionych stanowisk pracy oraz o czas trwania licencji. W ramach posiadanej licencji nie ma ograniczeń jeżeli chodzi o liczbę instalowanych serwerów typu „DLP Server" lub „Protector". Dzięki temu Forcepoint DLP nie ma licencyjnych ograniczeń wpływających na wydajność rozwiązania.

Ułatwiona metodologia wdrażania systemu DLP

Firma Forcepoint proponuje następujący sposób postępowania podczas wdrażania systemu Forcepoint DLP.

Metodologia P^3: nadawanie priorytetu działaniom mającym na celu identyfikację informacji

Wiele organizacji ma kłopoty z określeniem sposobu w jaki powinny podejść do spraw zapobiegania wyciekowi informacji. Forcepoint korzysta z metodologii P3, nadawania priorytetu działaniom prowadzącym do ustanowienia systemu identyfikacji informacji. Metodologia P3 skład się z trzech elementów:

- **Informacje najważniejsze**

  Określ najważniejsze informacje w swojej organizacji. Te 1 do 5% informacji jest najbardziej kluczowy, a dostęp do nich ma być najbardziej zastrzeżony. Właściciele powinni znać dokładne rozmieszczenie najważniejszych informacji oraz wiedzieć jakie systemy kontroli zapobiegają ich utracie. Firmy muszą nadać tym kluczowym informacjom cyfrowe „odciski palca", przypisać im właścicieli oraz ustalić odpowiadające im polityki bezpieczeństwa.

- **Zgodnie z zasadą Pareto**

  Następnie ustal, które 20% informacji biznesowych reprezentuje 80% wartości. Te powszechnie używane informacje na ogół rezydują w kilku istotnych źródłach danych. Wrażliwym informacjom należącym do tej klasy powinny być nadane cyfrowe „odciski palca" wraz z określeniem ich właścicieli oraz specyficznych reguł dotyczących ich dystrybucji.

- **Progresywność**

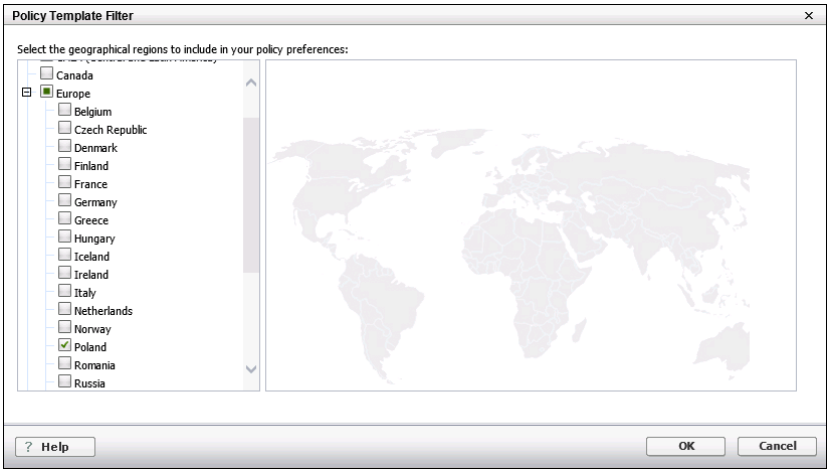
  W końcu określ zasoby informacji, które mają być chronione z niższym priorytetem. Informacje są często chronione fazami, w których etapowo dodawane są pewne typy zasobów informacji.

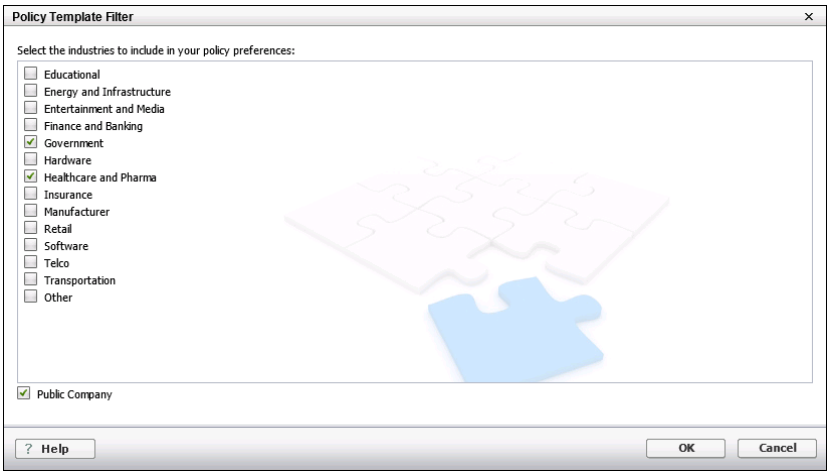
Zapoczątkowanie projektu zapobiegania utracie informacji może wydawać się przytłaczające, ale metodologia P^3 pomaga organizacjom nadać priorytet tym obszarom, na których powinny skupić się ich działania.

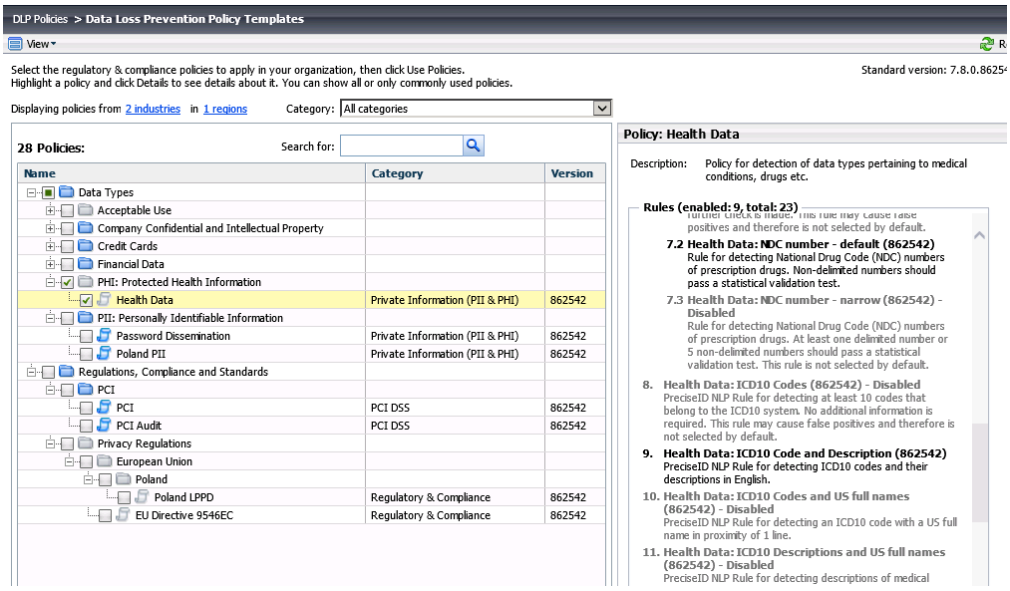
Predefiniowane szablony polityk

Rozwiązanie Forcepoint DLP dysponuje bardzo dużą liczbą (obecnie ok. 1600) gotowych szablonów standardowych polityk. Szablony te bardzo ułatwiają implementację systemu DLP w szczególności jeżeli chodzi o realizację narzuconych rekomendacji i standardów.

Szablony polityk są w przypadku produktu Forcepoint posegregowane w taki sposób, że wystarczy wybrać odpowiedni kraj i sektor, by otrzymać przejrzystą listę tych polityk, które będą najbardziej przydatne.





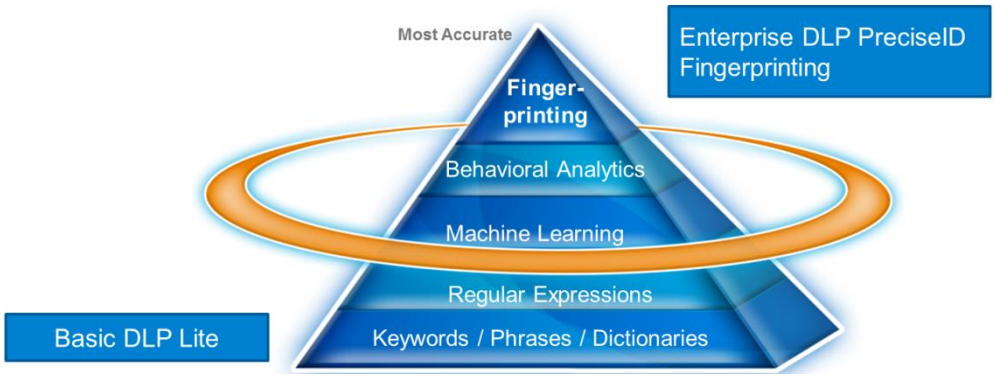


W ramach oferowanych szablonów znajduje się wiele polityk, które są przygotowane specjalnie z myślą o rynku polskim. Chodzi tutaj o wzorce pozwalające np. wykrywać numery PESEL, NIP, REGON czy numery dowodu osobistego. Tego rodzaju szablony są wynikiem współpracy z istniejącymi już klientami na rynku polskim. Support Forcepoint wprowadza do produktu nowe szablony również na prośbę klientów.

Z relacji klientów firmy Forcepoint wynika, że polityki oparte o gotowe szablony stanowią często ok. 80% zaimplementowanych polityk.

Efektywne i precyzyjne metody oznaczania danych

Rozwiązanie Forcepoint DLP pozwala na klasyfikację i wykrywanie informacji w oparciu o bardzo efektywne mechanizmy



Oprócz technik stosunkowo prostych jak słowa kluczowe, słowniki lub wyrażenia regularne, DLP oferuje bardzo wyrafinowane techniki jak:

- reguły NLP (Natural Language Processing)
- File Fingerprinting (PeciseID)
- Database Fingerprinting (PeciseID)
- Machine Learning

Zaawansowane metody i technologie wykrywania informacji są ważne z dwóch powodów:

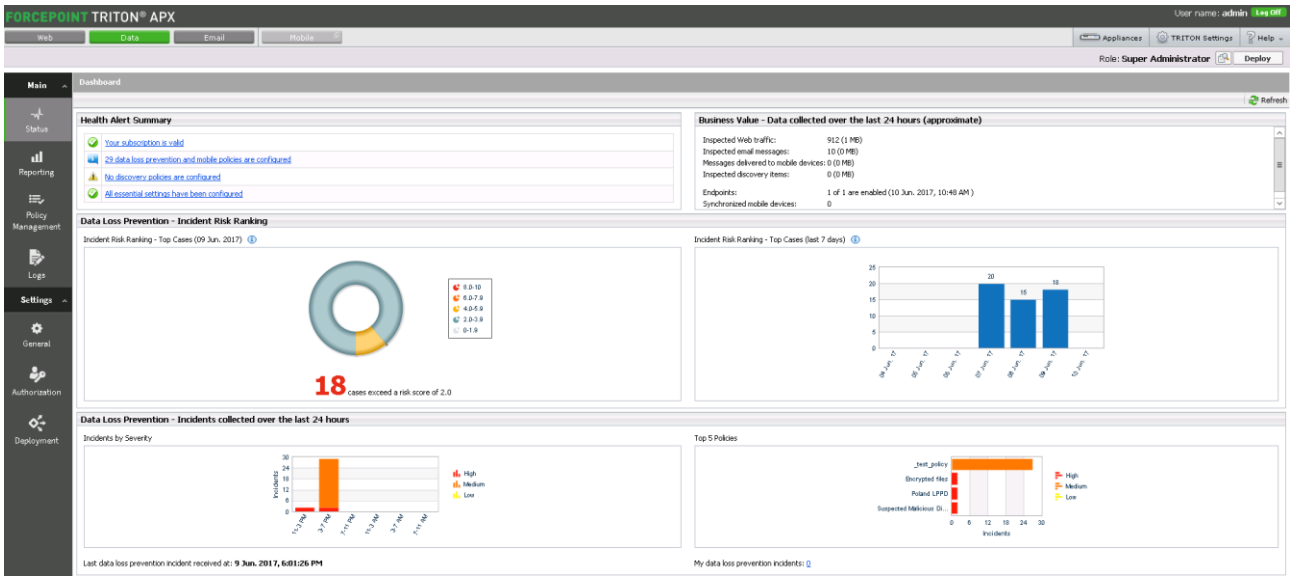
1. Pozwalają w prosty sposób definiować reguły polityki DLP (np. bezpośrednio zasobu sieciowego, z SharePointa lub bezpośrednio z bazy danych)
2. Precyzja generowanych incydentów przekłada się w sposób bezpośredni na efektywność całego systemu, ponieważ nadmierna ilość incydentów fałszywych (false-positive) ma dramatyczny wpływ na ilość potrzebnych zasobów administracyjnych. Zbyt duża liczba incydentów może w skrajnych przypadkach spowodować, że system DLP zostanie zaniechany. Należy pamiętać o tym, że administrator systemu w ciągu dnia pracy jest w stanie przeanalizować i realizować tylko ograniczoną liczbę incydentów.

Elastyczność i spójność implementowanych reguł DLP

Forcepoint DLP jest również rozwiązaniem, które oferuje mocne ramy budowania i wymuszania polityk dla użytkowników, danych, punktu docelowego transferu informacji i formy komunikacji. Dzięki temu możliwe jest jasne i precyzyjne określenie tego: **kto** może przesłać **jakie dane, gdzie** i za pomocą jakiego **kanału komunikacyjnego**:

Reguły polityk budowane w systemie Forcepoint DLP są wspólne dla części sieciowej i hostowej rozwiązania. Jeżeli administrator nie ograniczy tych reguł w sposób celowy, będą one miały zasięg globalny i będą działać dla wszystkich modułów rozwiązania.

System Forcepoint jest zarządzany centralnie przez Web GUI (Triton Manager). Triton Manager jest również wykorzystywany przez pozostałe rozwiązania firmy Forcepoint (Web Security oraz Email Security)



Forcepoint DLP Endpoint

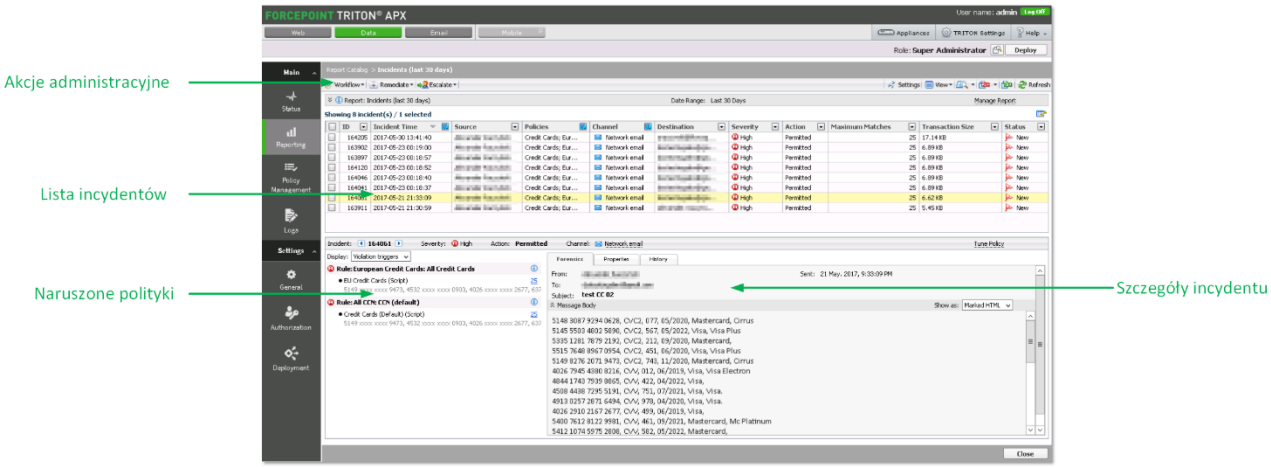
Forcepoint DLP Endpoint jest składnikiem tzw. hostowego DLP. W przypadku Endpointa firmy Forcepoint należy wspomnieć o kilku cechach, które go wyróżniają.

1. **Forcepoint DLP Endpoint jest zasilany politykami, które są budowane centralnie.** Nie ma potrzeby budowania oddzielnych reguł dla sieciowego i hostowego DLP.
2. **Endpoint firmy Forcepoint może być oferowany w języku polskim.** Ma to szczególne znaczenie w przypadku użytkowników, którzy nie muszą władać językiem obcym, a **muszą** stasować się do obowiązujących reguł ochrony informacji.
3. **Forcepoint DLP Endpoint posiada własny silnik analizy polityk.** Dlatego też działanie Endpoint'a nie jest uzależnione od połączenia z centralnym systemem zarządzającym. Endpoint potrafi wykryć wyciek i wykonać poprawna akcję również wtedy, gdy komputer użytkownika jest off-line.

Proste administrowanie incydentami

Dużą część pracy z wdrożonym już systemem DLP stanowi zarządzanie incydentami generowanymi przez użytkowników. Dlatego ułatwienie zadań administracyjnych w tym zakresie zwiększa z znaczącym stopniu przydatność rozwiązania dla celów organizacji.

Administrator systemu DLP posiada w przypadku rozwiązania Forcepoint narzędzia, które implementują gotowy workflow do obróbki incydentów.



Administrator incydentu ma do dyspozycji szczegółowe informacje na temat incydentu łącznie z kopią samego dokumentu czy wiadomości email (forensics data). W ramach oferowanego rozwiązania administrator może zmienić status incydentu, może również zmienić jego priorytet i zakwalifikować go według ustalonych reguł i poddać dalszej obróbce. Tego rodzaju działania na wygenerowanych incydentach mogą być wykonane ręcznie z poziomu konsoli zarządzającej lub mogą być zautomatyzowane. Podjęte akcje są logowane w systemie i historii incydentu.

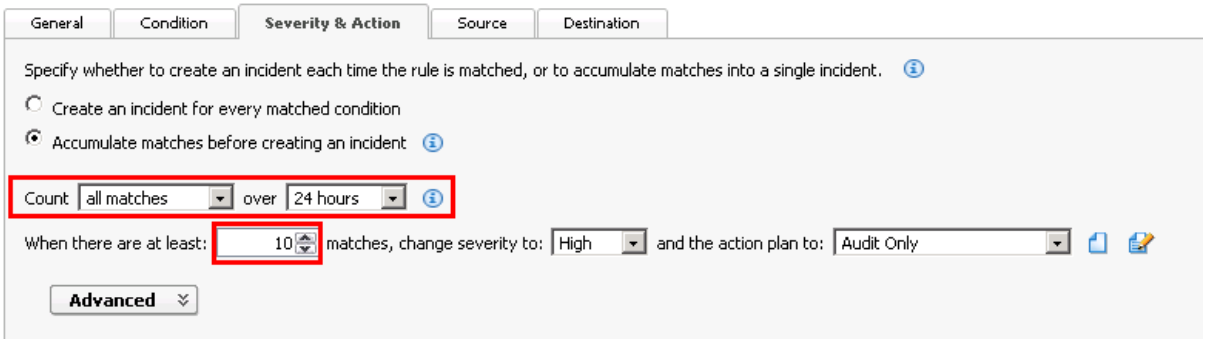
Należy pamiętać o tym, że sprawne zarządzaniami incydentami jest w rzeczywistości jednym z podstawowych warunków powodzenia projektu DLP w organizacji.

Drip DLP

Bardzo często reguły DLP są budowane w oparciu o progi graniczne. Przykładowo pojedynczy numer NIP nie jest informacją poufną. Jednak dokument zawierający kilkadziesiąt takich numerów NIP, może nieść ze sobą ryzyko utraty pakietu informacji istotnych.

Systemy DLP umożliwiają budowanie reguł, które wykrywają wzorce tylko po przekroczeniu takich progów granicznych. Fakt ten można jednak wykorzystać i wysyłać dane małymi porcjami. Istnieje wiele przykładów oprogramowania złośliwego, które działa właśnie w taki sposób.

Forcepoint DLP oferuje budowania reguł, które uwzględniają progi graniczne działające w określonym czasie, a nie tylko w przypadku jednorazowego wycieku. Taka reguła uniemożliwia porcjowanie wycieków informacji ważnych:



Funkcjonalność ta jest wyjątkowa dla systemu Forcepoint DLP.

Technologia OCR

Forcepoint DLP oferuje również możliwość analizy informacji zawartej w plikach graficznych. Chodzi tutaj przede wszystkim o uniemożliwienie wycieku informacji poprzez zrzuty ekranu. Informacja z plików graficznych jest ekstrahowana za pomocą technologii OCR i następnie poddana analizie przez zdefiniowane reguły polityki.

Technologia ta jest oferowana z powodzeniem dla części sieciowej rozwiązania Forcepoint DLP.

Integracja systemu Forcepoint DLP z innymi rozwiązaniami firmy Forcepoint

Rozwiązanie Forcepoint DLP integruje się z rozwiązaniami innych producentów. W szczególności istniej możliwość integracji z rozwiązaniami typu proxy lub ochrony poczty elektronicznej.

Firma Forcepoint oprócz technologii DLP oferuje również własne rozwiązanie w zakresie Web Security oraz Email Security. Jest rzeczą oczywistą, że integracja w ramach produktów jednego producenta odbywa się w sposób jeszcze bardziej bezproblemowy i dający dodatkowe efekty synergii.

- Zarówno rozwiązanie Web Security jak również rozwiązanie Email Security firmy Forcepoint są zaopatrzone w silniki analityczne polityk DLP. Stąd też wypływające informacje nie muszą być przekazywane do analizy lecz są analizowane bezpośrednio na rozwiązaniu proxy lub na bramce poczty elektronicznej.
- Integracja rozwiązania Forcepoint DLP z rozwiązaniem Forcepoint Web Security umożliwia dodanie politykom DLP świadomości kontekstowej w zakresie kategorii URL. Taka świadomość kontekstowa umożliwia przykładowo rozróżnienie wycieku informacji na witryny o charakterze finansowym od takich samych wycieków na witryny phishingowe.
- Rozwiązanie Forcepoint Web Security jest rozwiązaniem typu proxy, które dodatkowo umożliwia rozszywanie ruchu SSL. Stąd też analiza ruchu HTTPS w zakresie wycieku informacji jest p przypadku integracji obu produktów znacznie ułatwiona.

Korzyści związane z zastosowaniem technologii Forcepoint DLP

Technologia DLP pozwala sprostać nowym wymaganiom i ryzykom związanymi z nowymi technologiami IT oraz ze sposobem pracy użytkowników.

Technologia DLP pozwoli na monitorowanie przysyłania kluczowych informacji takich jak:

- Dane osobowe pracowników
- Dane osobowe klientów
- Dane dot. transakcji organizacji
- Wewnętrznych i poufnych dokumentów dotyczących planowanych produktów, kampanii reklamowych, nowych ofert itd.
- Dokumentów o fuzjach, przejęciach, cennikach, planowanych strategiach
- Innych...

Informacje te powinny bezwzględnie podlegać ochronie zarówno ze względu na wymagania prawne, którymi są one obłożone, jak i ze względu na ich ogromną wartość. Ich ochrona jest podstawowym powodem wprowadzenia systemu DLP.

Wprowadzenie systemu ochrony przed wyciekiem informacji przynosi jednak ze sobą dodatkowe korzyści:

1. Posiadanie wiedzy na temat tego gdzie przechowywane są informacje kluczowe organizacji, na temat tego jak są one używane i wykorzystywane pozwala na zmniejszenie ryzyka związanego z ryzykiem ich utraty czy niewłaściwego wykorzystania.
2. Wygenerowanie w systemie raporty pozwalają na zaplanowanie optymalnych procesów biznesowych związanych z użyciem informacji.
3. System DLP pozwala na wypełnienie norm i regulacji. Wiele typów informacji podlega takim regulacjom i ich wypełnienie jest lub w najbliższym czasie będzie obowiązkowe. (ochrona danych osobowych, PCI etc.). Niewypełnienie tych norm umożliwia grozi poniesieniem kosztów kar.
4. Wiele z polityk dotyczących korzystania z informacji jest trudnych do realizacji lub niemożliwych do przeprowadzenia. System DLP umożliwia definiowanie tych polityk na poziomie dopuszczalnego sposobu korzystania z informacji.