Forcepoint DLP i Forcepoint DLP Endpoint

UZYSKAJ WIDOCZNOŚĆ ORAZ KONTROLĘ W CELU ZABEZPIECZENIA SWOICH

FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP i Forcepoint DLP Endpoint

NIEZRÓWNANA WIDOCZNOŚĆ I KONTROLA NAD TWOIMI ISTOTNYMI DANYMI WSZĘDZIE TAM, GDZIE JEST TO KONIECZNE - W BIURZE, W DRODZE LUB W CHMURZE

Twoje najważniejsze dane są mobilne, przechowywane i dostępne w usługach typu chmura, takich jak Office 365 i Box w celu zachęcenia do współpracy kontrahentów na całym świecie. Forcepoint DLP jest wiodącym w branży rozwiązaniem DLP zapewniającym widoczność i kontrolę w celu ochrony danych niezależnie od tego, czy są one przechowywane i dostępne na urządzeniach mobilnych, takich jak komputery z systemem Windows i Apple, czy też udostępniane za pośrednictwem poczty elektronicznej oraz IM.

Chroń swoje dane wrażliwe niezależnie od miejsca ich użytkowania- na punktach końcowych, w chmurze lub lokalnie za pomocą Forcepoint DLP.

Forcepoint DLP akredytuje Twoją organizację

- Szybko sprostaj globalnym i branżowym wymaganiom dotyczącym zgodności z przepisami określonymi w ramach zdefiniowanych reguł, które są utrzymywane i aktualizowane przez wyznaczony zespół badawczy Forcepoint.
- Wykorzystaj narzędzia do klasyfikacji danych w celu identyfikacji i ochrony własności intelektualnej bez względu na to, gdzie są przechowywane.
- Reguła behawioralna łączy zawartość i świadomość kontekstu w celu automatycznego wykrywania zachowań wysokiego ryzyka przez użytkowników, np. przesyłanie wiadomości e-mail na konta osobiste lub pakowanie danych przy użyciu szyfrowania w celach eksfiltracji.
- Łatwe znajdowanie i zabezpieczanie plików zapisanych na urządzeniach końcowych Mac, Windows i Linux
- Identyfikacja i zapobieganie utracie danych w usługach chmury takich jak Office 365 i Box
- Wdrożenie skutecznych kontroli dostępu i kompleksowego audytu w celu sprostania wymaganiom wewnętrznym i zewnętrznym.
- Bezproblemowe zintegrowanie się z rozwiązaniami zabezpieczeń danych stosowanymi przez osoby trzecie z Microsoft, HP, Splunk, IBM, Titus, Boldon James i Citrix.
- Analityka DLP, która wykorzystuje modelowanie danych i analizę statystyczną w celu automatycznego identyfikowania zachowania użytkowników stanowiących największe ryzyko utraty danych lub kradzieży. Dzięki takiemu rozwiązaniu zespół ds. bezpieczeństwa może wykorzystać doświadczenie ekspertów Forcepoint.
- Architektura TRITON Forcepoint umożliwia ujednolicenie rozwiązań zabezpieczających, koordynowanie reguły ochrony, pozwala na podzielenie się informacjami w wielu punktach i korzystanie z scentralizowanego zarządzania w zakresie ochrony Twoich danych.

Kluczowe funkcje

- **IIncident Risk Ranking** wykorzystuje zaawansowane analizy danych, aby zapewnić zespołowi ds. operacji zabezpieczających raport o największych zagrożeniach związanych z bezpieczeństwem danych w Twojej organizacji.
- **Zintegrowane OCR** identyfikuje poufne dane i znaczniki IP w obrazach, takich jak projekty CAD, zeskanowane dokumenty, MRI i zrzuty ekranu.
- **Drip DLP** analizuje skumulowaną aktywność transmisji danych w czasie w celu wykrycia niewielkich ilości wycieku danych
- **Reguła behawioralna** łączy w sobie świadomość kontekstu i treści w celu automatycznego określenia, kiedy dane wrażliwe są narażane przez użytkowników.
- **Nasz unikatowy system PreciseID Fingerprinting** może wykryć częściowy ślad danych strukturalnych (zapisy bazy danych) lub niestrukturalnych (dokumenty) w punktach końcowych systemu Mac i Windows - niezależnie od tego, czy pracownik pracuje w biurze czy poza siecią.
- **Automatyczne szyfrowanie danych** przekazywanych na przenośnych urządzeniach pamięci masowej w celu zapewnienia bezpiecznego udostępniania danych partnerom.
- **Zdarzenie wynikające z przepływu pracy związane z pocztą elektroniczną** ułatwia rozpowszechnianie zdarzenia w celu przeglądu i naprawy przez właścicieli danych i interesariuszy biznesowych, bez konieczności udostępniania systemu zarządzania DLP.
- **Wykrywanie i zapobieganie wysyłaniu danych wrażliwych** przez organizację za pośrednictwem poczty e-mail, przesyłanie przez sieć, klientów usług IM chmury- zawiera wewnętrzne szyfrowanie SSL zarówno dla ruchu sieciowego jak i punktu końcowego.
- **Zainstalowanie składników DLP w Microsoft** w celu zastosowania reguły DLP w programie Microsoft Office 365.

„Forcepoint DLP było najpewniejszym rozwiązaniem, jakie znaleźliśmy w zakresie zatrzymania i zapobiegania wyciekom danych”

— Amir Shahar, Manager ds. Zabezpieczania Informacji, Cellcom Israel Ltd.

Forcepoint DLP Capabilities

PRZYJMIJ INNOWACJE Z ZAUFANIEM

Spełnienie potrzeb klientów i pozostawanie konkurencyjnym wymaga innowacji i zapewnienia pracownikom dostępu do nowych technologii. Rozwiązanie DLP firmy Forcepoint rozszerza kontrolę zabezpieczeń danych w aplikacji chmury dla firm i na urządzeniach końcowych. Pozwala to bezpiecznie korzystać z potężnych usług chmury, takich jak Microsoft Office 365, Google for Work i SalesForce.com, a także chronić poufne dane i własność intelektualną na laptopach z systemem Windows i Mac, zarówno w sieci, jak i poza nią.

Forcepoint umożliwia bezpieczne dzielenie się i kooperację danych wewnątrz organizacji jak i poza nią. Dzięki szyfrowaniu poufnych danych przesyłanych na przenośnych urządzeniach pamięci masowej, które są automatycznie rozszyfrowywane w punktach końcowych dzięki Forcepoint DLP Endpoint, dostęp do danych mają wszyscy zaufani partnerzy.

ZŁAGODŹ UCIĄŻLIWOŚCI ZWIĄZANE Z WDRAŻANIEM I ZARZĄDZANIEM

Oferujemy najbardziej precyzyjne i dokładne reguły Enterprise DLP z najprostszymi regułami wdrażania dowolnego dostawcy DLP. Nasza biblioteka reguły globalnej i przyjazny dla użytkownika kreator korzysta z filtrów regionalnych i branżowych w celu polecenia takiego zestawu reguł DLP, który szybko zabezpieczy własność intelektualną i dane regulowane (wszystko w jednym szablonie). Forcepoint jest również pierwszym dostawcą usług DLP, który udostępnia strategie dotyczące zachowań, które łączą w sobie świadomość treści i kontekstu w celu automatycznego określenia, kiedy użytkownicy są narażeni na wrażliwe dane. Zdarzenie wynikające z przepływu pracy związane z pocztą elektroniczną ułatwia rozpowszechnianie zdarzenia w celu przeglądu i naprawy danych przez ich właścicieli i interesariuszy, bez konieczności wymagania dostępu do systemu zarządzania DLP. Usatysfakcjonuj audytorów ujednoliconymi raportami, umożliwiając ich dostosowywanie w miarę potrzeby.

PEŁNA OCHRONA DANYCH Z NAJBARDZIEJ ZAAWANSOWANYMI TECHNOLOGIAMI PRZEMYSŁOWYMI

Złośliwy zrzut ekranu zapisany jako plik jpeg, obrazy medyczne, obrazy bankowe lub starsze dokumenty zeskanowane i zapisywane jako obrazy przedstawiają martwe punkty dla tradycyjnych rozwiązań DLP - ale nie dla Forcepoint DLP.

Dzięki zastosowaniu OCR Forcepoint(Optycznego Rozpoznawania Znaków) możesz wiarygodnie identyfikować i zabezpieczyć poufne dane wewnątrz obrazu. Ta wyjątkowa możliwość pozwala kontrolować przepływ informacji poufnych w zrzutach ekranów, faksach, smartfonach i tabletach, a także w dokumentach, takich jak kontrolowane, pokwitowane i zeskanowane pliki, zabezpieczając przed atakami i zagrożeniami wewnętrznymi związanymi z kradzieżą danych.

Uzyskaj lepszą widoczność i dostrzeż zaawansowane taktyki kradzieży danych, takich jak niestandardowe szyfrowanie w celu zaciemnienia danych lub przesyłanie danych w małych ilościach, aby uniknąć wykrycia.

POWIĄZANIE PRZEPŁYWU DANYCH Z ZACHOWANIEM UŻYTKOWNIKA W ZAKRESIE BEZPIECZEŃSTWA OCHRONY DANYCH

Forcepoint jest pierwszym dostawcą, który zintegrował nasze zaawansowane rozwiązanie DLP z Forcepoint Insider Threat w celu zapewnienia kontekstu w zakresie naruszeń reguł danych i dokumentowania zamiarów użytkowników. To wiodące połączenie zapewnia kontekst w zakresie prób użytkownika dotyczących przekazania poufnych danych.

Widok „zza ramienia” polegający na przechwytywaniu i odtwarzaniu DVR zapewnia niezbędny kontekst dotyczący aktywności użytkownika i Twoich danych, identyfikując wczesne sygnały ostrzegawcze naruszonego systemu, skradzionych poświadczeń, użytkowników nieuczciwych lub popełniających błędy.

Komponenty Forcepoint DLP i Forcepoint DLP Endpoint

Połączenie Forcepoint DLP (Forcepoint DLP Discovery i Forcepoint DLP Network) z Forcepoint DLP Endpoint rozszerza kontrolę Enterprise DLP Forcepoint na kanały, które stanowią największe zagrożenie dla Twoich danych: www, e-mail, aplikacje chmury i punkty końcowe. Forcepoint jest jedynym dostawcą, który zapewnia strategie i technologie klasy korporacyjnej w celu zapewnienia zabezpieczenia zintegrowanych kanałów (www i poczty elektronicznej) i realizacji tych reguł i raportów w zakresie rozwiązań Enterprise DLP, zapewniając jednocześnie najbardziej zaawansowaną technologię w branży, zabezpieczającą najważniejsze dane. PreciseID Fingerprinting może wykryć nawet fragment strukturalnych lub niestrukturalnych danych lokalnych, umieszczonych w chmurze lub w punkcie końcowym Windows lub Mac, w sieci lub poza nią.

FORCEPOINT DLP ENDPOINT	Forcepoint DLP Endpoint chroni najważniejsze dane w punktach końcowych systemu Windows i Mac w sieci firmowej i poza nią. PreciseID Fingerprinting umożliwia wykrycie nawet fragmentu strukturalnych lub niestrukturalnych danych w punkcie końcowym zlokalizowanym poza siecią. Monitoruj przesyłanie danych przez sieć (w tym HTTPS), a także przesyłanie do usług chmury, takich jak Office 365 i Box Enterprise. Pełna integracja z programem Outlook, Notes i klientami poczty e-mail, wszystko przy użyciu tego samego interfejsu użytkownika, co rozwiązania Forcepoint's Data, Web, Email i Endpoint.
FORCEPOINT DLP DISCOVERY	Forcepoint DLP Discovery identyfikuje i zabezpiecza poufne dane w sieci, a także dane przechowywane w usługach chmury, takich jak Office 365 i Box Enterprise. Po dodaniu Forcepoint DLP Endpoint, moc Forcepoint DLP Discovery można rozszerzyć do punktów końcowych systemu Mac OS X i Windows zlokalizowanych w sieci i poza nią. Wykorzystaj najnowocześniejszą technologię w branży w celu zagwarantowania, że Twoje dane wrażliwe nie zostaną naruszone.
FORCEPOINT DLP NETWORK	Istotne jest, aby zatrzymać kradzież danych podczas ich przemieszczania przez e-mail i kanały sieciowe. Forcepoint DLP Network pomaga w identyfikacji i zapobieganiu przypadkom działania złośliwego oprogramowania i przypadkowej utracie danych podczas ataków zewnętrznych lub rosnących zagrożeń wewnątrz sieci użytkownika. Licznik zaawansowanych technik unikania zagrożeń wyposażony w skuteczne OCR (Optical Character Recognition) umożliwia rozpoznawanie danych na obrazie. Użyj Drip DLP w celu zatrzymania kradzieży danych pojedynczego zapisu i monitorowania zachowania w celu identyfikacji użytkownika wysokiego ryzyka.
IMAGE ANALYSIS MODULE	W celu sprostania wymaganiom prawnym obowiązującym w wielu częściach świata lub po prostu zapewnienia odpowiedniego środowiska, opcjonalny moduł analizy obrazów identyfikuje wyraźne obrazy, takie jak pornografia przechowywana w sieci organizacji lub przemieszczana przez e-mail lub kanały internetowe. W celu uzyskania wersji demonstracyjnej wejdź na stronę forcepoint.com/contact

„Śpię lepiej, gdy wiem, że nasze dane są chronione przez Forcepoint."

— Ahmet Taskeser, Starszy lider SIMM, Finansbank

Siła płynąca z rozwiązań Forcepoint

Forcepoint Advanced Classification Engine (ACE)

Dzięki zastosowaniu złożonych ocen ryzyka i analizy predykcyjnej w celu zapewnienia najbardziej skutecznego zabezpieczenia, Forcepoint ACE zapewnia wbudowaną ochronę kontekstową w czasie rzeczywistym w zakresie sieci, poczty elektronicznej, danych i urządzeń przenośnych. Zapewnia również skuteczną regułę powstrzymywania poprzez analizę ruchu przychodzącego i wychodzącego z funkcją definiowania danych w celu zapobiegania kradzieży danych mających kluczowe znaczenie w branży. Klasyfikatory do ochrony w czasie rzeczywistym oraz analizy danych i zawartości (wynik wielu lat badań i rozwoju) umożliwiają firmie ACE wykrycie większej liczby zagrożeń, niż w przypadku tradycyjnych silników antywirusowych (korekta jest nanoszona codziennie pod adresem http://securitylabs.forcepoint.com). ACE jest podstawową ochroną wszystkich rozwiązań Forcepoint i jest obsługiwane przez Forcepoint ThreatSeeker Intelligence.

ZINTEGROWANE ZESTAWIENIE OBSZARÓW OCENY OCHRONY MOŻLIWOŚCI W OBRĘBIE 8 KLUCZOWYCH OBSZARACH

- 10.000 analizowanych szczegółów wspomagających dogłębną kontrolę.
- Predyktywny mechanizm zabezpieczeń przewiduje kilka ruchów do przodu.
- Obsługa wewnętrzna nie tylko monitoruje, ale blokuje zagrożenia.

Forcepoint ThreatSeeker Intelligence

Forcepoint ThreatSeeker Intelligence, zarządzane przez Forcepoint Security Labs, dostarcza podstawowych informacji o bezpieczeństwie dla wszystkich produktów bezpieczeństwa Forcepoint. Łączy ponad 900 milionów punktów końcowych, w tym dane wejściowe z serwisu Facebook, zaś dzięki zabezpieczeniom Forcepoint ACE analizuje do 5 miliardów żądań dziennie. Ta rozległa wiedza na temat zagrożeń bezpieczeństwa umożliwia ThreatSeeker Intelligence Cloud oferowanie aktualizacji zabezpieczeń w czasie rzeczywistym, które blokują zaawansowane zagrożenia, złośliwe oprogramowanie, ataki phishingu, przynęty i oszustwa, a także oferuje najnowsze rankingi sieciowe. ThreatSeeker Intelligence Cloud jest niezrównane pod względem wielkości i wykorzystuje ochronę ACE w czasie rzeczywistym w celu analizy zbiorczych danych wejściowych. (Po uaktualnieniu do programu Web Security, Forcepoint ThreatSeeker Intelligence pomaga zmniejszyć ryzyko wystąpienia zagrożeń internetowych i kradzieży danych).

TRITON Architecture

Dzięki najlepszemu w swojej klasie zabezpieczeniu i ujednoliconej architekturze, TRITON Architecture oferuje ochronę w czasie rzeczywistym z wbudowanymi funkcjami ochrony Forcepoint ACE. Niespotykane zabezpieczenia w czasie rzeczywistym ACE są wspierane przez Forcepoint ThreatSeeker Intelligence i wiedzę specjalistów z Forcepoint Security Labs. Wynikiem jest skomasowana architektura z ujednoliconym interfejsem użytkownika i informacjami dotyczącymi bezpieczeństwa.

KONTAKT
www.forcepoint.com/contact

FORCEPOINT
POWERED BY Raytheon

www.forcepoint.com