Forcepoint Web Security

BEZPIECZEŃSTWO CHMURY ORAZ LOKALNEJ SIECI

FORCEPOINT
POWERED BY Raytheon

Forcepoint Web Security

BEZPIECZEŃSTWO CHMURY ORAZ LOKALNEJ SIECI

Twoja firma oraz jej dane są obiektem ciągłych ataków. Tradycyjne rozwiązania bezpieczeństwa nie zapewniają już wystarczającej ochrony. W rzeczywistości mogą powodować zagrożenie utratą danych i sporami sądowymi. Ochrona sieci i danych przed zaawansowanymi zagrożeniami, pakietami crypto-ransomware i zestawami exploitów ma kluczowe znaczenie dla przetrwania firmy w coraz bardziej ryzykownym świecie cyfrowym obejmującym telefony komórkowe i chmury.

Możliwość dostosowania za pomocą możliwości rozszerzenia

Firmy potrzebują dostosowywanych rozwiązań, które komunikują się wzajemnie, aby zapewnić sobie ochronę przed takimi rodzajami zagrożeń, jakie mają miejsce obecnie. Forcepoint Web Security zapewnia ochronę w czasie rzeczywistym przed zaawansowanymi zagrożeniami i kradzieżą danych oferując wiele możliwości rozwoju i modułów dostosowujących pakiet ochrony sieci do potrzeb Twojej organizacji.

Forcepoint Web Security zapewnia silną ochronę dzięki skutecznym informacjom o defektach oraz wykrywaniu i monitorowaniu aplikacji w chmurze, zmniejszając tym samym zagrożenie dla poufnych danych zarówno w środowisku lokalnym, jak i w obszarze użytkowników telefonów komórkowych.

Co najważniejsze, Forcepoint Web Security łatwo integruje się z innymi rozwiązaniami Forcepoint zapewniając jednolity, spójny mechanizm zabezpieczający, który może chronić przed zagrożeniami przychodzącymi i wychodzącymi nawet przy bardzo małym zespole zajmującym się ochroną.

Cele zabezpieczenia sieci

Większość współczesnych rozwiązań zabezpieczających nie jest przystosowanych do zaawansowanych zagrożeń. Forcepoint Web Security jest zaawansowaną, operującą w czasie rzeczywistym ochroną przed zagrożeniami.

ZABEZPIECZENIE KAŻDEGO UŻYTKOWNIKA, WSZĘDZIE TAM, GDZIE ISTNIEJE NIEBEZPIECZEŃSTWO ZAAWANSOWANYCH ZAGROŻEŃ

Rozszerz swoją ochronę, zarówno lokalnie jak i w obrębie wszystkich pracowników zdalnych wszędzie tam, gdzie mają dostęp do sieci.

IDENTYFIKACJA I KONTROLOWANIE ZAGROŻEŃ ZWIĄZANYCH Z CIENIAMI APLIKACJI I USŁUGAMI CHMURY

Odkryj aplikacje chmury używane w organizacji. Monitoruj ich wykorzystanie w celu określenia i blokowania tych, które stanowią największe zagrożenie.

ZMNIEJSZ SWOJE WYDATKI NA ZABEZPIECZANIE SIECI, POPRAWIAJĄC WYDAJNOŚĆ OPERACYJNĄ

Wzmocnij produkty zabezpieczające łącząc je na jednej platformie oraz zapewniając spójne elementy kontrolne bezpieczeństwa sieci, danych i aplikacji w chmurze. W łatwy sposób rozszerz swoje bezpieczeństwo poprzez dodanie sandobxu chmury, DLP, wykrywanie zagrożeń i bezpieczeństwo dla urządzeń mobilnych.

„Forcepoint pomogło nam zmienić sposób myślenia na bardziej konstruktywny i wykorzystać więcej aplikacji w chmurze w celu poprawy wyników biznesowych.”

— Chris Anderson, Dyrektor ds. Usług Infrastrukturalnych, Bendigo and Adelaide Bank

Forcepoint Web Security

ANALIZA W CZASIE RZECZYWISTYM W CELU ZAPEWNIENIA ZAAWANSOWANEJ OCHRONY PRZED ZAGROŻENIAMI

Dzięki ośmiu obszarom oceny obrony, przy użyciu procesu obliczania złożonego z analizą predykcyjną Forcepoint ACE, Forcepoint Web Security wykracza poza zakres zwykłej ochrony antywirusowej. Wieloskładnikowe silniki treści analizują w czasie rzeczywistym pełną treść strony internetowej, aktywne skrypty, linki internetowe, profile kontekstowe, pliki i pliki wykonywalne.

ŁATWY DOSTĘP DO PULPITU NAWIGACYJNEGO ZAGROŻEŃ DANYCH

Zaawansowany pulpit nawigacyjny zagrożeń stworzony przez Forcepoint Web Security zawiera raporty dotyczące osób, które zostały zaatakowane oraz tego, jakie dane były celem, docelowy punkt końcowy danych oraz sposób ataku. Zdarzenia związane z bezpieczeństwem obejmują przechwytywanie w miarę możliwości skradzionych danych. Ochrona sieci obejmuje komunikaty przychodzące i wychodzące.

ZINTEGROWANA OCHRONA PRZED KRADZIEŻĄ DANYCH

Wiodące w branży zintegrowane zabezpieczenia przed kradzieżą danych (opcjonalne) wykrywają i przechwytują próby kradzieży danych oraz zapewniają zgodność z przepisami w zakresie zapobiegania ich utracie (DLP). Przykłady takich funkcji obejmują wykrywanie zaszyfrowanych plików wideo, kradzież plików z hasłami, powolne wycieki danych (Drip-DLP), optyczne rozpoznawanie znaków OCR (Optical Character Recognition) tekstu w obrazach i świadomości miejsca docelowego.

ZINTEGROWANY SANDBOXING

Dowiedz się w jaki sposób lepiej chronić zasoby swojej firmy, dzięki automatycznej analizie zachowania złośliwego oprogramowania wraz ze zintegrowaną usługą sandbox.

ODKRYWANIE, MONITOROWANIE ORAZ KONTROLA APLIKACJI CHMURY

Odkryj aplikacje chmury używane w Twojej organizacji i uniemożliwiaj użytkownikom narażanie się na niebezpieczeństwo danych poprzez ich wysyłanie do nieobsługiwanych aplikacji i usług chmury.

Udoskonalone moduły ochrony

HYBRID CLOUD DEPLOYMENT	**Rozszerzona ochrona sieci i egzekwowanie polityki w stosunku do użytkowników zdalnych** Wdrożenie Forcepoint Web Security jako fizycznego lub wirtualnego urządzenia do prywatnej chmury. Każdą z opcji można rozszerzyć o globalną infrastrukturę chmury Forcepoint w celu ochrony użytkowników zdalnych.
WEB DLP	**Dodaj potężny, kontekstowy mechanizm DLP zapewniający dodatkową ochronę przed kradzieżą danych** Forcepoint Web DLP zapewnia ochronę przed kradzieżą danych i umożliwia zgodność z przepisami w zakresie ponad 1700 wstępnie zdefiniowanych zasad i szablonów. Obejmuje również wiodącą w branży ochronę Drip-DLP przeciwko powolnym wyciekom danych, Optical Character Recognition (OCR) przeciwko kradzieży plików danych w plikach graficznych lub Custom Encryption Detection w celu wykrycia plików zaszyfrowanych.
CLOUD SANDBOX	**Integracja sandboxingu behawioralnego do automatycznej oraz ręcznej analizy plików złośliwego oprogramowania** Analizuj podejrzane pliki w środowisku wirtualnym, zaś w celu zapewnienia najwyższego poziomu ochrony przed złośliwym oprogramowaniem wykorzystaj możliwość znacznie głębszego wglądu, niż w przypadku prostego wykonywania plików. Po wykryciu złośliwych plików, wszystkie szczegółowe raporty kryminalistyczne są automatycznie udostępniane.
MOBILE SECURITY	**Rozszerzona polityka i ochrona użytkowników iOS i Android** Rozszerz istniejącą politykę bezpieczeństwa na urządzenia mobilne i chroń je przed zaawansowanymi zagrożeniami, złośliwym oprogramowaniem mobilnym, atakami typu phishing, fałszowaniem oraz innymi zagrożeniami. Program Forcepoint Mobile Security współpracuje z menedżerem urządzeń przenośnych (MDM) w celu zapewnienia ich pełnej ochrony.

Pozostałe możliwości

ZDALNA OCHRONA UŻYTKOWNIKA

Zarządzaj użytkownikami korporacyjnymi, branżowymi i zdalnymi za pomocą jednej konsoli i polityki obejmującej wdrożenie chmury hybrydowej.

ELASTYCZNA INSPEKCJA SLL

Rozszerzone funkcje inspekcji SSL umożliwiają monitorowanie ruchu HTTPS przy jednoczesnym zachowaniu prywatności i wymogów prawnych.

API DLA INFORMACJI O ZAGROŻENIACH

Wydane API ułatwia zachowanie bezpieczeństwa twojej sieci poprzez wdrożenie przemysłowej lub charakterystycznej dla poszczególnych regionów informacji o zagrożeniach oraz umożliwienie zautomatyzowania zarządzania bezpieczeństwem.

KONTROLA APLIKACJI ORAZ PROTOKOŁU

Agent sieciowy zapewnia precyzyjną kontrolę nad setkami protokołów i aplikacji zwiększających bezpieczeństwo.

ELASTYCZNE RAPORTOWANIE

Cztery konfigurowalne pulpity nawigacyjne, a także ponad 60 wstępnie zdefiniowanych i dostosowanych raportów, zapewniają łatwe do zrozumienia informacje techniczne oraz dotyczące działalności, a także cenne informacje na temat poziomów zagrożeń i nie tylko.

OPCJE WIELOTOROWEGO ROZWOJU

Wybierz sposób rozwoju za pomocą chmury, urządzeń hybrydowych lub lokalnych (wirtualnych lub fizycznych).

OCHRONA PROXY-LESS ENDPOINT

Nasze rozwiązanie chroni użytkowników pracujących w dowolnej sieci, w dowolnym miejscu. Aplikacje nadal działają w środowiskach, które zazwyczaj powodują problemy z rozwiązaniami w obrębie serwera proxy.

ZINTEGROWANY DLP INCIDENT RISK RANKING

Pierwsze w branży rozwiązanie analityczne dotyczące bezpieczeństwa, obniża koszty i zwiększa wydajność weryfikacji DLP.

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 politykę 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