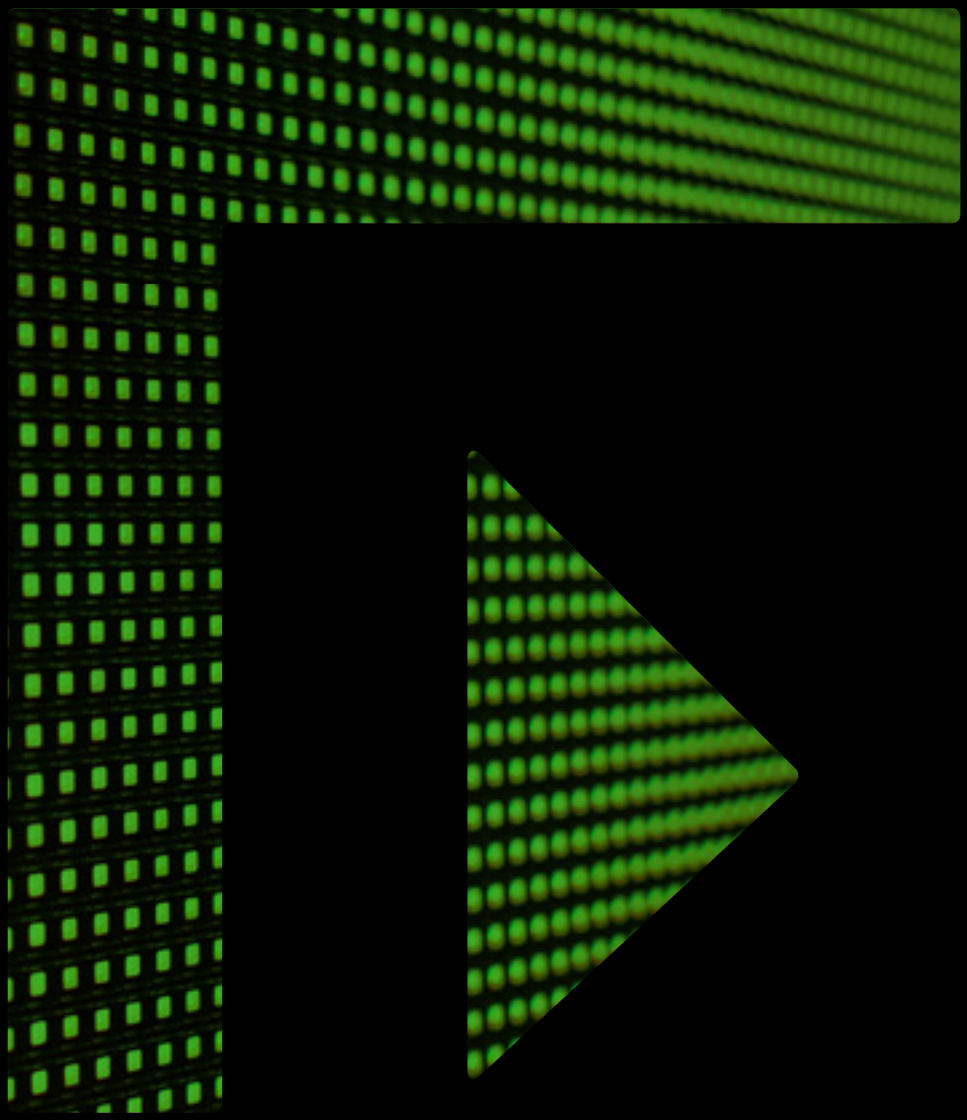


Forcepoint Email Security

CHMURA FORCEPOINT ORAZ LOKALNE ZABEZPIECZENIE POCZTY E-MAIL

FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security

CHMURA FORCEPOINT ORAZ LOKALNE ZABEZPIECZENIE POCZTY E-MAIL

Większość cyberataków pochodzi z poczty e-mail i wykorzystuje zaawansowane, skoordynowane taktyki, takie jak przynęty zaprojektowane społecznie i ukierunkowany phishing. Ponieważ te wielostopniowe zagrożenia łączą w trakcie ataków elementy sieci i wiadomości e-mail, stanowią one tzw. „Kill Chain" możliwości powstrzymania ich jeszcze przed doprowadzeniem do naruszenia.

Maksymalizuj swoje wykorzystanie i bezpieczeństwo poczty elektronicznej

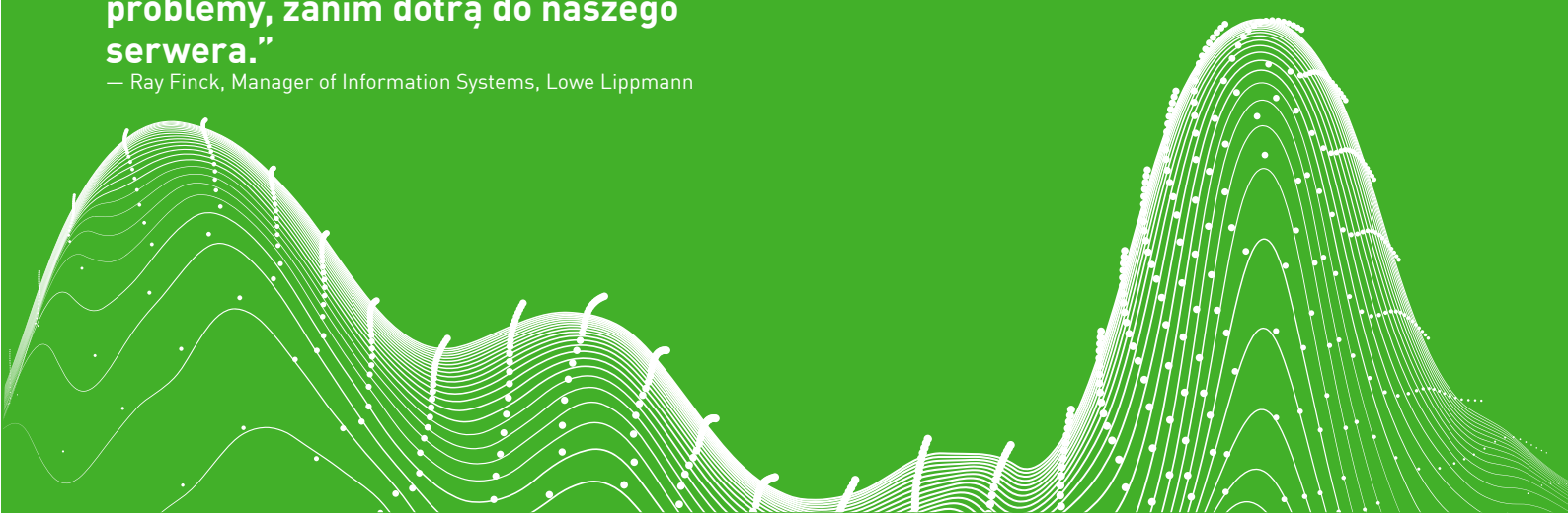
Forcepoint Email Security identyfikuje ukierunkowane ataki, użytkowników wysokiego ryzyka i wewnętrzne zagrożenia, upełnomocniając jednocześnie pracowników mobilnych i `vwychodzących lub próby komunikacji botnetowej, Forcepoint Email Security zabezpiecza mieszane środowiska za pomocą ochrony świadomej zawartości, chroniąc komunikację poczty elektronicznej w ramach kompletnego i powiązanego systemu ochrony przeciwko zaawansowanym zagrożeniom (ang. Advanced Persistent Threats - APT) oraz innym rodzajom zaawansowanych zagrożeń.

Wyzwania związane z zabezpieczeniem poczty e-mail

- APT wykorzystuje zwykle pocztę elektroniczną do wczesnych etapów zaawansowanych ataków.
- Poczta elektroniczna musi spełnić więcej wymogów, aby rozwiązać problem kradzieży danych i zagrożeń wewnętrznych.
- Firmy korzystają z usługi Office 365 i innych usług opartych na chmurze w celu zapewnienia rozwoju i w związku z wzajemną konkurencją.
- Ryzykowne nawyki użytkowników mogą prowadzić do naruszeń bezpieczeństwa i utraty danych.

„Ostatecznie jesteśmy bardzo zadowoleni z produktów Forcepoint. Forcepoint Email Security wykonuje swoje zadanie i rozwiązuje wszelkie problemy, zanim dotrą do naszego serwera."

— Ray Finck, Manager of Information Systems, Lowe Lippmann



Możliwości Forcepoint Email Security

ZATRZYMANIE APT ORAZ POZOSTAŁYCH ZAAWANSOWANYCH I UKIERUNKOWANYCH ZAGROŻEŃ

Advanced Classification Engine(ACE) firmy Forcepoint stanowi rdzeń wszystkich rozwiązań Forcepoint. ACE identyfikuje złośliwe przynęty, zestawy exploitów, pojawiające się zagrożenia, łączność z botnetami i inne zaawansowane zagrożenia w ramach Kill Chain. Pozwala to na identyfikację wczesnych etapów ataku przez Forcepoint Email Security. Może nawet identyfikować zagrożenia z wykorzystaniem złośliwego oprogramowania na poziomie zero-day, korzystając z zaawansowanych możliwości oceny, obejmujących w pełni zintegrowane sandboxowe zachowanie plików.

ZABEZPIECZENIE DANYCH WRAŻLIWYCH PRZED ATAKAMI ZEWNĘTRZNYMI ORAZ ZAGROŻENIAMI WEWNĘTRZNYMI

W celu przygotowania się na złośliwe zagrożenia wewnętrzne lub potencjalnie skuteczny cyberatak ważne jest, aby monitorować komunikację wychodzącą. Jest to konieczne zarówno w celu spełnienia wymagań dotyczących kradzieży danych, jak i wymagań biznesowych. Jedynie Forcepoint dostarcza technologię pozwalającą powstrzymać infiltrację oraz eksfiltrację danych za pomocą takich funkcji, jak:

- Skanowanie w formacie OCR (Optical Character Recognition) w celu zidentyfikowania poufnych danych ukrytych w obrazach, takich jak zeskanowane dokumenty lub zdjęcia z ekranu.
- Wykrywanie zaszyfrowanych plików w celu rozpoznawania niestandardowych zaszyfrowanych plików mających na celu zignorowanie identyfikacji.
- Monitorowanie ochrony przed utratą danych spływających (DLP) w celu określenia lokacji wyciekania poufnych danych w niewielkich ilościach.
- Zaawansowana analiza złośliwych plików i makr typowo wbudowanych w pliki MS Office.

BEZPIECZEŃSTWO ZAADOPTOWANIA TECHNOLOGII CHMURY, TAKICH JAK OFFICE 365 I BOX ENTERPRISE, W RAMACH WSPIERANIA MOBILNYCH ZASOBÓW ROBOCZYCH

Działy IT są zobowiązane do utrzymania obecnych systemów, przy jednoczesnym wspieraniu coraz bardziej mobilnej siły roboczej i stawianiu czoła wymaganiom związanym z wprowadzaniem nowych technologii, takich jak Office 365. Forcepoint Email Security zapewnia wiodące w branży mechanizmy, które wykorzystują systemy i inne informacje do kontroli komunikacji, na przykład uniemożliwiając całkowity dostęp do poufnych załączników e-mail na wrażliwych urządzeniach przenośnych, a jednocześnie umożliwiają pełny dostęp do całkowicie zabezpieczonych laptopów. Te zabezpieczenia przychodzące i wychodzące są obsługiwane w pakiecie Office 365.

IDENTYFIKACJA UŻYTKOWNIKA „WYSOKIEGO RYZYKA" I EDUKACJA UŻYTKOWNIKÓW W CELU POPRAWY ŚWIADOMOŚCI

Zasobne zbiory danych w programie Forcepoint Email Security są wykorzystywane w ramach wielu polityk w zakresie raportowania i identyfikowania systemów, które mogą wymagać szczególnej uwagi IT. Generują raport dotyczący wskaźników kompromisu w celu zidentyfikowania zainfekowanych systemów i bardziej proaktywnych raportów dotyczących podejrzanych zachowań, w tym potencjalnych zagrożeń wewnętrznych, takich jak „niezadowoleni pracownicy". Możliwości związane z uzyskaniem opinii od użytkownika pomagają w zakresie doedukowania pracowników na temat tego jakie popełniają błędy, pomagając im lepiej poznać i zrozumieć najlepsze praktyki dotyczące poczty e-mail.

Udoskonalone moduły ochrony

OPTIONAL HYBRID CLOUD DEPLOYMENT	**Wykorzystaj globalne usługi chmury ForcePoint w zakresie wydajności i skalowalności** Połącz się z ochroną przed zagrożeniami wynikającymi z usług filtrowania, opartą na chmurze w celu zachowania przepustowości dzięki wiodącym w branży rozwiązaniom antyspamowym SLA. Moduł hybrydowy dodaje do rozwiązań w obrębie poczty e-mail sandboxing URL oraz edukację w zakresie phishingu.
EMAIL DLP	**Zablokuj kradzieże danych przy użyciu świadomego treści DLP przeznaczonego dla przedsiębiorstw** Przygotuj się na zagrożenia wewnętrzne oraz kradzież danych poprzez złośliwe oprogramowanie, osiągnij cele dotyczące zgodności, a następnie zminimalizuj ryzyko związane z informacjami osobistymi lub IP. Zaawansowane funkcje umożliwiają wykrycie kradzieży danych ukrytych w obrazach lub zaszyfrowanych plikach nawet, jeśli są przekazywane w małych ilościach w celu uniknięcia wykrycia.
CLOUD SANDBOX	**Integracja sandboxingu behawioralnego do automatycznej i ręcznej analizy plików złośliwego oprogramowania** Uzupełnij analitykę Forcepoint ACE za pomocą zintegrowanego sanboxingu pliku w celu zapewnienia dogłębnej inspekcji. Skorzystaj z analizy behawioralnej w wirtualnym środowisku, aby odkryć zachowanie złośliwego oprogramowania Zero-day oraz inne zaawansowane złośliwe oprogramowania. Przetestuj pliki automatycznie lub ręcznie, aby wygenerować szczegółowe analizy.
EMAIL ENCRYPTION	**Zapewnij poufność wrażliwym połączeniom** Moduł szyfrowania wiadomości e-mail Forcepoint jest technologią opartą na zasadach, które umożliwiają zabezpieczenia dostarczanej poczty elektronicznej. Eliminuje tradycyjne bariery kosztów i złożoności, oferując łatwą administrację, bez złożonego zarządzania kluczami lub dodatkowego sprzętu.
IMAGE ANALYSIS	**Identyfikuj wyraźne obrazy, aby zapewnić akceptowalne wykorzystanie i zgodność** Moduł analizy obrazu Forcepoint umożliwia pracodawcom podejmowanie proaktywnych działań w celu monitorowania, edukowania i egzekwowania polityki dotyczącej adresów e-mail firmy w odniesieniu do jawnych lub pornograficznych załączników w postaci zdjęć.

„Forcepoint Email Security było atrakcyjne, ponieważ przejęło kontrolę nad bezpieczeństwem poczty e-mail i zapewniło nam więcej korzyści, niż oczekiwaliśmy pod względem elastyczności i łatwości obsługi. Ogólnie, Forcepoint Email Security umożliwiło dostarczenie naszym użytkownikom bardziej elastycznej, profesjonalnej i opłacalnej obsługi."

— Martin Law, Dyrektor ds. IT, NCP

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

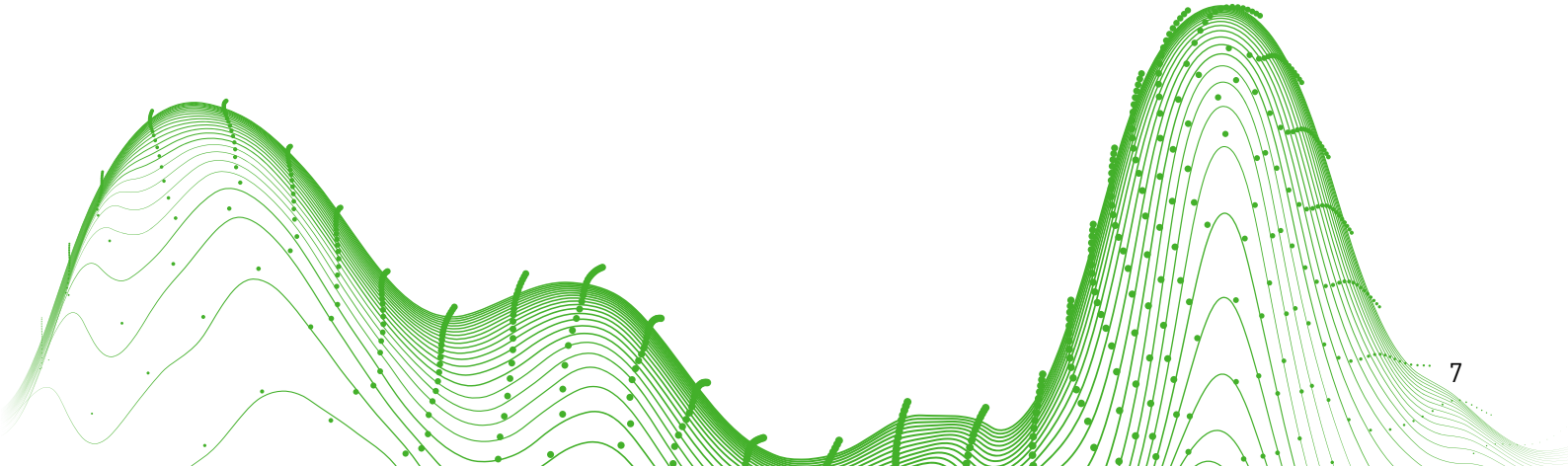
- 10.000 analizowanych szczegółów wspomagających dogłębną kontrolę.
- Predyktywny mechanizm zabezpieczeń przewiduje kilka ruchów do przodu.
- Obsługa wewnętrzna nie tylko monitoruje, ale blokuje zagrożenia.

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