TitanHQ SpamTitan PRIVATE CLOUD

BAKOTECH

SpamTitan Private Cloud

Filtrowanie wiadomości e-mail w oparciu o technologię chmury prywatnej. Usługa dla biznesu.

Wiele przedsiębiorstw skarży się na ciągle wzrastającą ilość spamu, który powoduje spadek poziomu usług i jest nośnikiem takich zagrożeń jak phishing czy infekcja złośliwym oprogramowaniem. Codzienne ataki niechcianych wiadomości powodują przeładowanie serwerów pocztowych, które nie są w stanie pracować efektywnie, zwiększają prawdopodobieństwo wystąpienia zagrożeń związanych z bezpieczeństwem oraz narażają firmy na straty wizerunkowe i finansowe.

Czym jest SpamTitan Private Cloud?

SpamTitan Private Cloud jest kompleksowym rozwiązaniem do ochrony poczty email, zapewniającym bezpieczeństwo firmy, pracowników oraz klientów, działającym w oparciu o technologię chmury.
Prywatna chmura może znajdować się w chmurze TitanHQ znajdującej się na terenie Polski, jak również we własnym centrum danych firmy. Jest ona niezwykle łatwa w obsłudze, a jednocześnie zapewnia wykrywanie spamu (z efektywnością 99.97%), blokowanie wirusów oraz złośliwego oprogramowania, daje możliwość uwierzytelniania, skanowania poczty wychodzącej, jak również udostępnia struktury umożliwiające efektywne raportowanie.
U podstaw wszystkich podejmowanych przez nas działań leży interes naszych klientów na całym świecie. Już dzisiaj dajemy Ci możliwość przetestowania naszych produktów za darmo i przekonania się, dlaczego tak wiele firm powierzyło nam zapewnienie bezpieczeństwa swojego biznesu.

Kontrola i ochrona treści wiadomości e-mail. Usługa dla biznesu.

SpamTitan zapewnia firmom ochronę przed zagrożeniami poprzez zarządzaniem pocztą e-mail oraz analizę wiadomości otrzymywanych przez pracowników, blokowanie spamu, wirusów i złośliwego oprogramowania.
SpamTitan Private Cloud jest idealnym rozwiązaniem dla dużych firm oraz dostawców usług internetowych, jako że gwarantuje wszelkie korzyści bram sieciowych bez konieczności przeznaczania dużych nakładów na zarządzanie. Wersja testowa SpamTitan Private Cloud może być przygotowana na zamówienie przez naszych inżynierów w ciągu 24 godzin.

Dlaczeg warto używać Spam Titan Private Cloud?

SpamTitan Private Cloud został stworzony specjalnie, aby realizować oczekiwania firm i dostawców usług internetowych w zakresie zapewnienia ochrony ich użytkowników i sieci przed spamem, wirusami i złośliwym oprogramowaniem.

Funkcjonalności rozwiązania

Zarządzanie
Możliwość własnego brandingu
Zmień branding rozwiązania poprzez umieszczenie logo swojej firmy oraz zmianę kolorów na kolory firmowe w celu sprzedania platformy jako usługi hostingowej.

Rozszerzone API
SpamTitan Private Cloud posiada rozszerzone API, co umożliwia integrację z zewnętrznymi produktami do zarządzania.

Skalowalność
SpamTitan Private Cloud jest produktem skalowalnym i w łatwy sposób może być rozbudowywany, w celu spełniania wymagań rozwijającej się firmy. Charakteryzuje się on możliwością obsługi nieograniczonej liczby użytkowników oraz nieograniczonej liczby domen. Umożliwia również administrowanie na wielu poziomach, włączając w to m.in. poziom użytkownika, jak również poziom domeny czy grup domen.

Nasza lub wasza chmura
Rozwiązanie SpamTitan Private Cloud jest instalowane jako usługa działająca w chmurze. SpamTitan Private Cloud może być hostingowana w chmurze TitanHQ jako dedykowana prywatna chmura lub w centrum danych dostawcy usług internetowych.

Pakiet raportów
SpamTitan Private Cloud może przesyłać użytkownikom raporty kwarantanny w ustalonym czasie i z ustaloną częstotliwością. Raporty kwarantanny zawierają listę wiadomości e-mail, które nie zostały przesłane do użytkownika z powodu pojawienia się podejrzenia, iż mogły zawierać niepożądane treści, takie jak spam czy wirusy. Użytkownik końcowy ma możliwość zadecydowania, czy tego rodzaju wiadomości mają zostać dostarczone do skrzynki odbiorczej, dodane do list bezpiecznych wiadomości czy też usunięte.

Funkcjonalności panelu użytkownika
Filtrowanie spamu
SpamTitan Private Cloud filtruje przepływ firmowych wiadomości e-mail w celu uniemożliwienia dostarczenia spamu do skrzynek użytkowników. Rozwiązanie gwarantuje 99.97% skuteczność wykrywania spamu dzięki wielopoziomowej analizie, na którą składają się: tworzenie i uaktualnianie czarnych list w czasie rzeczywistym (RBL), tworzenie list stron internetowych zawartych w niepożądanych wiadomościach e-mail (SURBL), tworzenie polityk umożliwiających wysyłanie wiadomości oraz analiza bayesowska. Wszystkie te elementy w połączeniu ze wskaźnikiem tzw. false-positive na poziomie 0.03% gwarantują kompleksowe zabezpieczenie przed niepożądanymi wiadomościami, a jednocześnie zapewniają, że użytkownicy nie utracą dostępu do istotnych wiadomości e-mail.

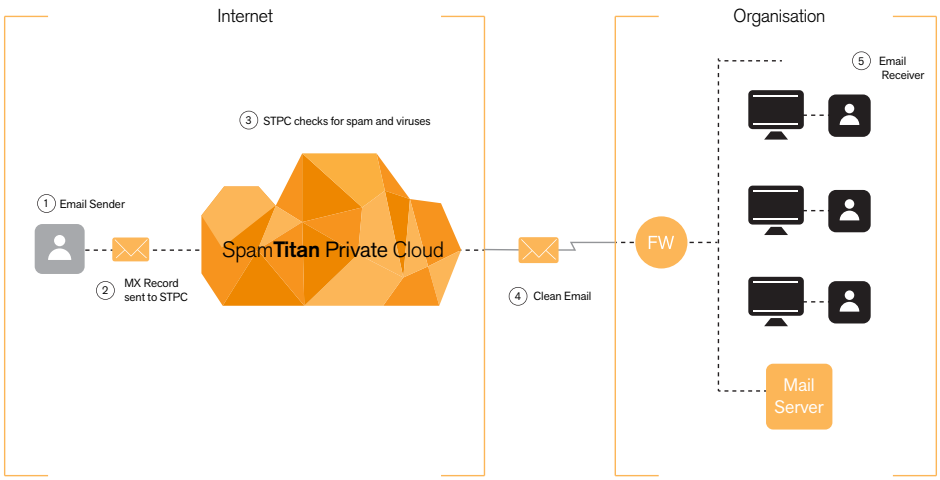
Blokowanie wirusów i złośliwego oprogramowania
Nasze wielokrotnie nagradzane rozwiązanie działa w oparciu o podwójne zabezpieczenie antywirusowe – Kaspersky Lab oraz Clam AV, które pozwalają na blokowanie wirusów oraz złośliwego oprogramowania, podejmujących próby zainfekowania sieci poprzez wiadomości e-mail.

Tworzenie białych i czarnych list
Rozwiązanie umożliwia tworzenie czarnych i białych list nadawców wiadomości e-mail, co oznacza, że sam możesz decydować o tym, że wiadomości z danego adresu mailowego będą zawsze dostarczane lub zawsze blokowane.

Weryfikacja odbiorcy
SpamTitan oferuje szereg możliwości weryfikacji odbiorcy, takich jak: dynamiczna weryfikacja odbiorcy (DRV), LDAP, weryfikacja w oparciu o listy czy weryfikacja specyficznych wyrażeń. W momencie kiedy wiadomość e-mail trafia do Spam Titan Private Cloud, jest ona poddawana weryfikacji na podstawie adresu e-mail, co prowadzi do odrzucenia niepożądanych e-maili i spamu.

Skanowanie poczty wychodzącej
Skanowanie wychodzących wiadomości e-mail jest niezwykle ważne. Uniemożliwia ono rozsyłanie wiadomości zawierających wirusy z kont firmowych, a tym samym chroni przed dodaniem adresu IP do czarnych list, tworzonych przez rozmaite serwisy na całym świecie. Dodanie adresu IP do czarnej listy powoduje niedostarczanie wiadomości e-mail, wpływa negatywnie na przebieg operacji biznesowych oraz efektywność działań, a proces usuwania adresu z czarnej listy jest skomplikowany i czasochłonny. Zadaniem SpamTitan Private Cloud jest niedopuszczenie do zaistnienia takiej sytuacji.

Uwierzytelnianie
Ustawienia uwierzytelniania sieci Web pozwalają na wybranie rodzaju uwierzytelniania, jaki będzie stosowany dla konkretnej domeny w momencie, kiedy użytkownik podejmie próbę logowania. Dostępne są następujące metody uwierzytelniania: wewnętrzna (domyślna), LDAP, serwerów SQL, POP3 oraz IMAP.
Wykorzystanie zewnętrznych modułów uwierzytelniających gwarantuje, że jeśli tylko jest to możliwe, użytkownik nie musi zapamiętywać szeregu różnych haseł, jako że wszelkie próby logowania będą przekierowywane do odpowiedniego dla danej domeny serwera uwierzytelniającego.



Specyfikacja techniczna

Filtrowanie spamu	» Rozwiązanie gwarantuje 99.97% skuteczność wykrywania spamu dzięki wielopoziomowej analizie, na którą składają się: ▪ Tworzenie i uaktualnianie czarnych list w czasie rzeczywistym (RBL), ▪ Tworzenie list stron internetowych zawartych w niepożądanych wiadomościach e-mail (SURBL), ▪ Tworzenie polityk umożliwiających wysyłanie wiadomości, ▪ Analiza bayesowska » Bardzo niski wskaźnik tzw. false positive, wynoszący 0.03%
Blokowanie wirusów i złośliwego oprogramowania	» SpamTitan Private Cloud działa w oparciu o podwójne zabezpieczenie antywirusowe – Kaspersky Lab oraz Clam AV, które pozwalają na blokowanie wirusów oraz złośliwego oprogramowania, podejmujących próby zainfekowania sieci poprzez wiadomości e-mail.
Tworzenie czarnych i białych list	» Możesz decydować o tym, że wiadomości z danego adresu mailowego będą zawsze dostarczane lub zawsze blokowane.
Raportowanie	» Raporty kwarantanny w ustalonym czasie i z ustaloną częstotliwością. Raporty te zawierają listę e-maili, które nie zostały przesłane do użytkownika z powodu podejrzenia, iż mogły zawierać spam lub wirusy. Użytkownik końcowy ma możliwość zdecydowania, czy tego rodzaju wiadomości powinny zostać dostarczone, dodane do list bezpiecznych wiadomości czy też usunięte.
Weryfikacja odbiorcy	» Ustawienia uwierzytelniania sieci Web pozwalają na wybranie rodzaju uwierzytelniania, jaki będzie stosowany dla konkretnej domeny w momencie, kiedy użytkownik podejmie próbę logowania. » Dostępne są następujące metody uwierzytelniania: ▪ Wewnętrzna (domyślna) ▪ LDAP ▪ Serwery SQL ▪ POP3 ▪ IMAP » Wykorzystanie zewnętrznych modułów uwierzytelniających gwarantuje, że jeśli tylko jest to możliwe, użytkownik nie musi zapamiętywać szeregu różnych haseł, jako że wszelkie próby logowania będą przekierowywane do odpowiedniego dla danej domeny serwera uwierzytelniającego.
Skanowanie poczty wychodzacej	» SpamTitan może również skanować pocztę wychodzącą, a tym samym zapobiegać sytuacji, w której adres IP znajdzie się na czarnej liście.
Możliwość własnego brandingu	» Zmień wizerunek platform poprzez umieszczenie logo firmy oraz zmianę kolorów na kolory firmowe w celu sprzedania jej jako usługi hostingowej.
Rozszerzone API	» SpamTitan Private Cloud posiada rozszerzone API, co umożliwia integrowanie z zewnętrznymi rozwiązaniami do zarządzania.
Skalowalność	» SpamTitan Private Cloud jest łatwo skalowalny i może być rozbudowywany wraz z rozwojem firmy. Charakteryzuje się on możliwością obsługi nieograniczonej liczby użytkowników i nieograniczonej liczby domen oraz umożliwia wielopoziomowe administrowanie, włączając w to poziom użytkownika oraz poziom domeny i grup domen itd.
Działający w chmurze	» Rozwiązanie SpamTitan Private Cloud jest instalowane jako usługa działająca w chmurze. SpamTitan Private Cloud może się znajdować w chmurze Titan HQ znajdującej się na terenie Polski jako dedykowana prywatna chmura lub w centrum danych dostawcy usług internetowych.

O firmie

O firmie

TitanHQ specjalizuje się w dostarczaniu rozwiązań biznesowych typu MAIL & WEB SECURITY, związanych z ochroną serwerów pocztowych, filtrowaniem ruchu sieciowego oraz zapewnianiem bezpieczeństwa dostarczanych treści, co pozwala chronić zasoby korporacyjne przed zagrożeniami z zewnątrz. Oprogramowanie antyspamowe SpamTitan oraz rozwiązanie do web filteringu WebTitan charakteryzuje wysoka skuteczność i efektywność kosztowa.

Celem TitanHQ jest dostarczenie klientom jak najprostszych zabezpieczeń internetowych i taki cel przyświecał firmie od momentu rozpoczęcia działalności w 1999 roku. Aktualnie sieć klientów obejmuje ponad 5000 firm w ponad 120 krajach.
TitanHQ jest prywatnym przedsiębiorstwem działającym w Irlandii i Stanach Zjednoczonych.

Bakotech Sp. z o.o. z siedzibą w Krakowie, jest częścią międzynarodowej grupy dystrybucyjnej Bakotech®. Jako specjalizowany dystrybutor rozwiązań IT w zakresie bezpieczeństwa, sieci i infrastruktury IT, spółka koncentruje się na dostarczaniu najwyższej jakości produktów i usług w centralnej i wschodniej Europie, w szczególności w: Polsce, Bułgarii, Rumunii, Słowacji, Chorwacji i na Węgrzech, a także w krajach nadbałtyckich. Firma zajmuje się sprzedażą w kanale partnerskim, poprzez rozbudowaną sieć partnerów. Bakotech posiada w swoim portfolio innowacyjne produkty, które odniosły sukces międzynarodowy, a dzięki dystrybutorowi wchodzą nie tylko na rynek polski, ale również krajów Europy Środkowo-Wschodniej.

Od 2014 roku Bakotech Sp. z o.o. jest wyłącznym, autoryzowanym dystrybutorem rozwiązań SpamTitan i WebTitan, umożliwiających ochronę serwerów pocztowych, bezpieczne przeglądanie stron www, kontrolę treści internetowych oraz ochronę firm przed szkodliwym oprogramowaniem i phishingiem.

Dane kontaktowe

BAKOTECH SP. Z. O.O.
ul. Św. Tomasza 34/B09
31-027 Kraków
e-mail: spamtitan@bakotech.pl, wsparcie@bakotech.pl
tel.: +48 12 376 95 08