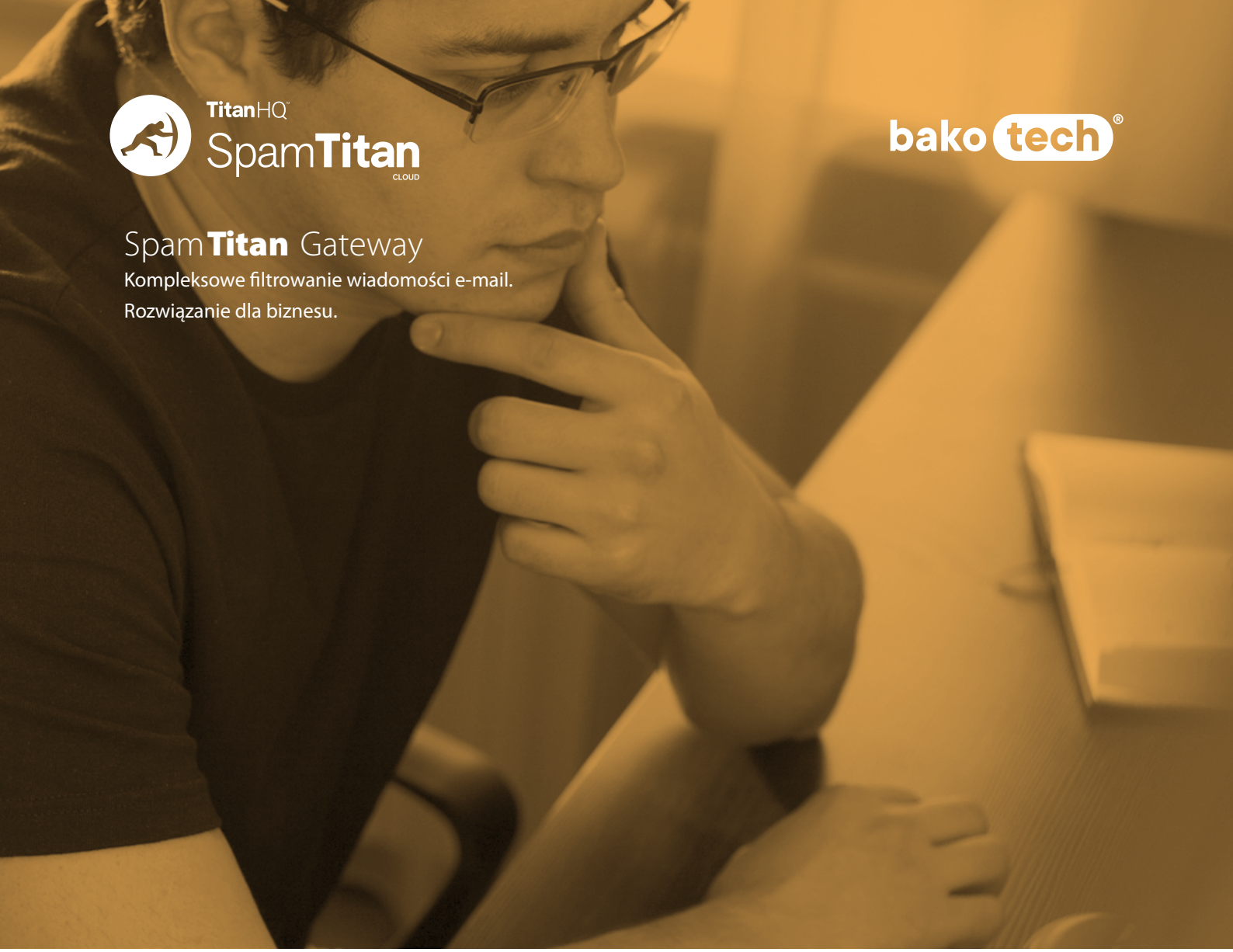

TitanHQ SpamTitan CLOUD

bako tech

SpamTitan Gateway

Kompleksowe filtrowanie wiadomości e-mail.
Rozwiązanie 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 Gateway?

SpamTitan Gateway jest kompleksowym rozwiązaniem bezpieczeństwa, chroniącym firmy, pracowników oraz klientów. Wdrożenie tego rozwiązania oraz zarządzanie nim jest niezwykle proste - SpamTitan Gateway jest rozwiązaniem typu software appliance; może zostać zainstalowane na urządzeniu lub działać w środowisku wirtualnym. Zapewnia, poza wieloma innymi funkcjonalnościami, 99.7% skuteczności w wykrywaniu spamu, a także blokowanie wirusów i złośliwego oprogramowania, możliwość uwierzytelnianie, skanowanie poczty wychodzącej oraz dostęp do skutecznych struktur raportowania.

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

SpamTitan chroni firmy przed zagrożeniami poprzez zarządzanie przepływem wiadomości e-mail, oraz analizowanie wiadomości otrzymywanych przez pracowników, blokowanie spamu, wirusów i złośliwego oprogramowania. Proces instalacji SpamTitan Gateway jest niezwykle prosty. Dodatkową zaletę stanowi doskonała integracja z istniejącą infrastrukturą.

Funkcjonalności rozwiązania

Filtrowanie spamu

SpamTitan Gateway filtruje firmowe wiadomości e-mail w celu zagwarantowania, że spam nie trafi do skrzynek odbiorczych pracowników. 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. Połączenie tych elementów ze wskaźnikiem tzw. false-positive na poziomie 0.03% pozwala zagwarantować, że użytkownicy nie stracą dostępu do istotnych wiadomości e-mail, a jednocześnie są w pełni chronieni przed spamem.

Blokowanie wirusów oraz złośliwego oprogramowania

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

Raportowanie

SpamTitan Gateway może przesyłać użytkownikom 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

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 SpamTitan Gateway, 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 Gateway 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.

Skalowalność

SpamTitan jest w pełni skalowalny, dla zapewnienia Twojej firmie najlepszej ochrony.

TitanHQ SpamTitan CLOUD

bako tech

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 Gateway działa w oparciu o podwójne zabezpieczenie antywirusowe Bitdefender 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	» SpamTitan oferuje szereg możliwości weryfikacji odbiorcy, takich jak: • Dynamiczna weryfikacja odbiorcy (DRV) • LDAP • Weryfikacja w oparciu o listy • Weryfikacja specyficznych wyrażeń Wszystko to gwarantuje poprawne wyliczenie liczby licencji. W momencie kiedy wiadomość e-mail trafi do SpamTitan, odpytany zostanie serwer poczty.
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 • 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 wychodzącej	» SpamTitan może również skanować pocztę wychodzącą, a tym samym zapobiegać sytuacji, w której adres IP znajdzie się na czarnej liście.

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. Drukarska 18/5,
30-348 Kraków

www.bakotech.pl
kontakt@bakotech.pl
+48 12 340 90 30