



Usługi szyfrujące Websense eliminują potrzebę utrzymywania systemów zarządzania kluczami oraz dodatkowej infrastruktury lub oprogramowania.

Websense Hosted Email Security Usługa szyfrowania

Szyfrowanie Websense to oparta o polityki usługa zabezpieczająca wymianę korespondencji poprzez email z partnerami biznesowymi i osobami indywidualnymi. Prosta administracja, brak skomplikowanego zarządzania kluczami oraz wyeliminowanie potrzeby instalowania dodatkowego sprzętu i oprogramowania likwidują zwyczajowe bariery związane z kosztem i złożonością uniemożliwiające wprowadzenie systemu szyfrowania poczty. Ponadto, pełna integracja z usługą Websense Hosted Email Security oznacza, iż nie rezygnujesz z inspekcji szyfrowanej korespondencji pod kątem szkodliwego oprogramowania oraz zawartych treści. Szyfrowanie Websense jest prostym i opłacalnym rozwiązaniem, które pomaga organizacjom sprostać regulacjom oraz chronić poufność wrażliwych informacji.

Jak to działa:

Websense obsługuje szyfrowanie komunikacji pomiędzy serwerami korzystając ze standardu Transport Layer Security (TLS) oraz szyfrowanie ad hoc typu park-and-pull dla komunikacji z osobami indywidualnymi. Polityki szyfrowania mogą być skonfigurowane w oparciu o nadawcę, odbiorcę, ustawienia

czułości oprogramowania Outlook lub słowo kluczowe w temacie wiadomości. Szyfrowanie może być łączone z filtrowaniem zawartości, w celu szyfrowania wiadomości email o określonej zawartości, takiej jak wrażliwe lub poufne informacje.

Szyfrowanie Websense zapewnia:

- **Automatyczne szyfrowanie ważnych wiadomości email**, umożliwiające spełnienie wymagań zgodności z obowiązującymi regulacjami oraz zabezpieczające Twoje poufne informacje.
- **Prostą konfigurację i zarządzanie** bez konieczności utrzymywania systemów zarządzania kluczami oraz dodatkowej infrastruktury lub oprogramowania.
- **Dostęp do systemu z poziomu przeglądarki internetowej** gwarantujący uniwersalną kompatybilność z urządzeniami przenośnymi, systemami operacyjnymi oraz systemami pocztowymi bez potrzeby instalowania dodatkowego oprogramowania.
- **Współpraca** ze standardowymi bramami poczty elektronicznej oraz protokołem szyfrowania TLS.
- **Kontrolę zawartości i skanowanie złośliwego oprogramowania** dla szyfrowanych wiadomości email, pozwalające blokować zagrożenia i zapobiegać utracie danych.

Szyfrowanie jest zawarte bez dodatkowej opłaty w Websense Hosted Email Security and Content Control - systemie bezpieczeństwa poczty i kontroli zawartości.

Websense, Inc.
San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

Websense UK, Ltd.
Reading, Berkshire UK
tel 0118.938.8600
fax 0118.938.8697
www.websense.co.uk

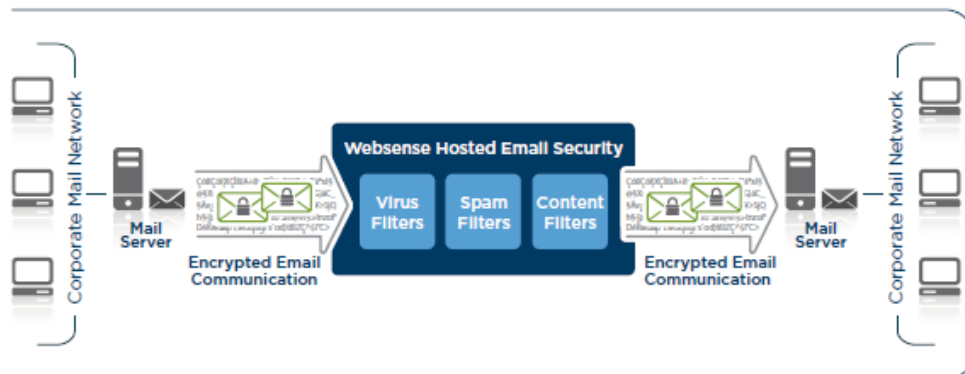
Dystrybucja w Polsce:

CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 012 378-37-00
tel. 012 632-51-66
tel. 012 292-75-22 ... 24
fax 012 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 032 444-65-11
tel. 032 203-92-35
tel. 32 609-80-50...51
fax 032 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 022 201-06-88
tel. 022 518-02-70...75
fax 022 518-02-73
e-mail: warszawa@clico.pl

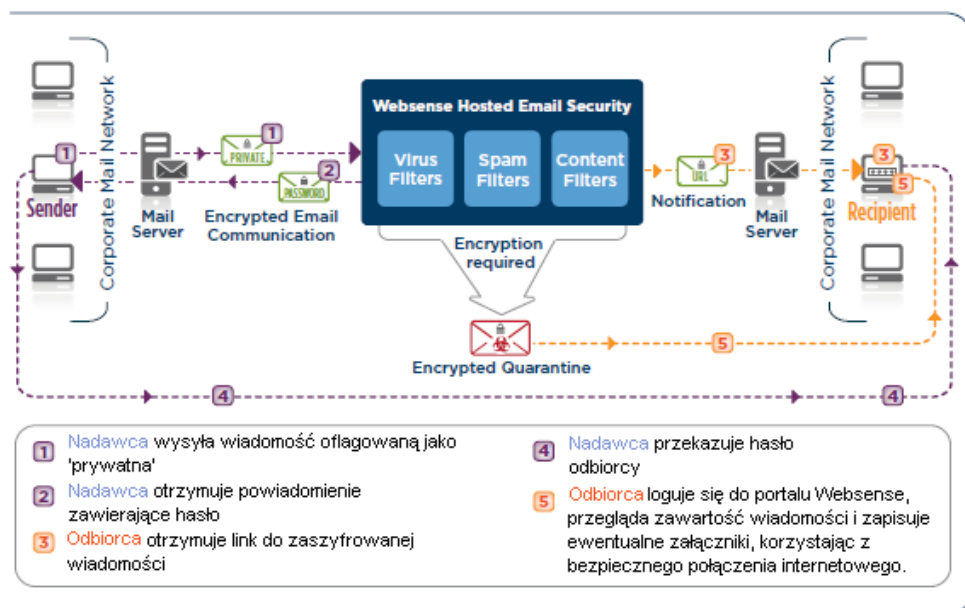
Szyfrowanie TLS



Proces szyfrowania TLS pomiędzy serwerami

Szyfrowanie pomiędzy serwerami przy użyciu protokołu TLS pozwala organizacjom na automatyczne szyfrowanie wiadomości email wysyłanych do określonych domen. Proces ten opiera się na ustanowieniu bezpiecznego, zaszyfrowanego tunelu pomiędzy serwerem poczty danej organizacji, centrum danych Websense oraz serwerem poczty odbiorcy. Szyfrowanie TLS, jeżeli tylko jest dostępne, jest wykorzystywane dla całej komunikacji, dodatkowo, może być wymagane dla określonych serwerów docelowych. Wymagana siła szyfrowania oraz parametry certyfikatów mogą być konfigurowane osobno dla każdego połączenia. Dzięki szyfrowaniu TLS organizacje mogą zabezpieczyć kanały komunikacji email z partnerami biznesowymi oraz ograniczyć przesyłanie wrażliwych informacji jedynie z wykorzystaniem chronionych kanałów.

Szyfrowanie typu Park-and-Pull



Proces szyfrowania typu park-and-pull

Szyfrowanie park-and-pull zabezpiecza pocztę email na podstawie polityki, nadawcy, grupy lub innych kryteriów, udostępniając zintegrowane narzędzia kontroli zawartości w celu szyfrowania i zapobiegania utracie wrażliwych danych. Szyfrowanie wysyłanych wiadomości może być inicjowane przez użytkowników końcowych lub egzekwowane zgodnie z globalnymi regułami szyfrowania. Podczas gdy zaszyfrowana wiadomość jest bezpiecznie przechowywana na serwerach Websense, odbiorca otrzymuje powiadomienie o jej wysłaniu. Dostęp do wiadomości uzyskiwany jest przez odbiorcę poprzez bezpieczne połączenie internetowe oraz przy użyciu hasła otrzymanego od nadawcy, co eliminuje konieczność utrzymywania złożonych systemów zarządzania i wymiany kluczy.