



Websense Hosted Email Security

Krajobraz obecnych zagrożeń poczty elektronicznej jest zdominowany przez zespolone ataki email i Web, gdzie ponad 85% niepożądanych wiadomości email zawiera w treści adresy URL. Dodatkowo organizacje stają przed problemem zwiększającego się ryzyka utraty danych oraz naruszania zasad regulujących korzystanie z poczty email. Należy przy tym zaznaczyć, że za wzrostem skomplikowania zagrożeń nie musi wcale podążać wzrost skomplikowania systemów zarządzania bezpieczeństwem.

Stworzony przez Websense i dostarczany jako usługa (z ang. software-as-a-service, SaaS) system bezpieczeństwa poczty elektronicznej łączy najlepsze technologie zabezpieczające informacje oraz środowisko Web z rozwiązaniami ochrony email. Dzięki temu jest w stanie zapewnić wgląd w nowopowstające zagrożenia oraz najwyższy poziom ochrony przed niebezpieczeństwami związanymi z wysyłaniem i odbieraniem wiadomości email. To proste w obsłudze rozwiązanie gwarantuje precyzyjną ochronę przed spamem, wirusami, spyware'em, phishingiem oraz zespolonymi zagrożeniami email i Web. Predefiniowane słowniki zawartości pomagają w upraszczaniu procesów zapobiegania utracie danych, spełniania norm oraz egzekwowania polityk dotyczących dopuszczalnego korzystania z poczty elektronicznej.

„Dzięki posiadanemu systemowi bezpieczeństwa poczty elektronicznej w formie usługi [Websense Hosted Email Security], zmniejszamy obciążenie wewnętrznych serwerów i eliminujemy potrzebę codziennego zarządzania systemami bezpieczeństwa email.”

Terry Kemp

Dyrektor Infrastruktury

Członek Zarządu Okręgowej Służby Zdrowia

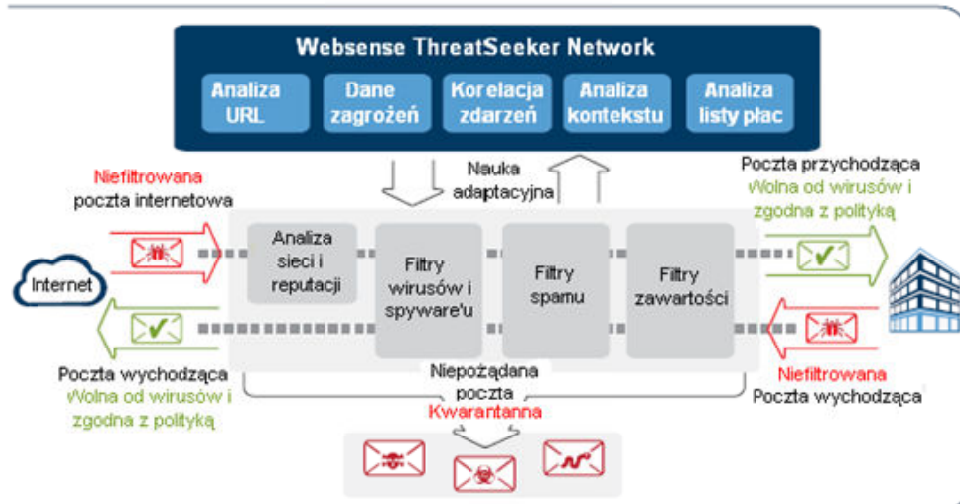
Jak to działa:

Ochrona poczty przy użyciu systemu bezpieczeństwa Websense SaaS jest prosta. Wystarczy skierować rekordy MX do centrów danych Websense, a całość poczty email będzie filtrowana jeszcze zanim dostanie się do sieci, oszczędzając miejsce na serwerze poczty oraz przepustowość. Centra danych Websense znajdują się w 10 lokalizacjach na całym świecie i zbudowane zostały na bazie

klastrowej, redundantnej architektury, zapewniającej wysoką dostępność (HA) oraz równowagę obciążenia (*load balancing*). Usługa zapewnia dostępność rzędu 99,999 procent, co poparte jest umowami dotyczącymi jakości usług (SLA), oraz certyfikatem ISO27001, co gwarantuje najwyższy poziom globalnego i lokalnego bezpieczeństwa, prywatności oraz poufności.

System bezpieczeństwa poczty elektronicznej Websense SaaS pozwala klientom:

- **Zmniejszyć koszty i złożoność prowadzonej działalności** poprzez brak konieczności instalowania lub obsługi jakiegokolwiek sprzętu w siedzibie przedsiębiorstwa, zwiększenie dostępnej przestrzeni dyskowej, wzrost przepustowości oraz zmniejszenie ogólnych kosztów administracyjnych.
- **Poprawić poziom bezpieczeństwa** dzięki wiodącemu systemowi ochrony przed zespolonymi zagrożeniami email i Web, wspartemu najwyższej jakości usługami (SLA) oraz możliwościami sieci Websense ThreatSeeker.
- **Zachować kontrolę** dzięki zapewnieniu dostępu do systemu 24 godziny na dobę, 7 dni w tygodniu oraz udostępnieniu elastycznych opcji dostosowywania polityk, ustawiania konfiguracji, zarządzania kwarantanną i raportowania.



Zarys usługi Hosted Email Security

„Wraz z uruchomieniem usługi Websense Hosted Email Security zniknął problem spamu”

Lee Smith
Dyrektor Operacyjny IT
Harvey Nichols

Możliwości systemu Hosted Email Security

Pakiety Email Hosted Security	Anty-spam	Antywirus	Filtry zawartości	Szyfrowanie
Hosted Antispam	•			
Hosted Email Security	•	•		
Hosted Email Security and Content Control	•	•	•	•

Anty-spam

Websense zapewnia wysoce precyzyjny system blokowania spamu z bardzo niskim odsetkiem błędnie sklasyfikowanych wiadomości (false positives), poparty gwarancją 99% skuteczności wykrywania spamu zawartą w umowie SLA. Przy identyfikowaniu spamu system korzysta z szeregu technologii, takich jak reputacja nadawcy, techniki adaptacyjnego uczenia się, analiza URL-i, heurystyka, cyfrowe odciski palca oraz optyczne rozpoznawanie spamu obrazkowego. Co najważniejsze jest to jedyne rozwiązanie oferujące zintegrowaną, wiodącą na rynku technologię bezpieczeństwa Web firmy Websense w celu zapewnienia ochrony przed phishingiem oraz zespolonymi zagrożeniami email oraz Web. Każda wiadomość email jest oceniana, a następnie wynik jest porównywany z progiem zdefiniowanym przez klienta w celu ustalenia, jakie działanie powinno zostać podjęte.

Antywirus

Przychodzące i wychodzące wiadomości email są skanowane w poszukiwaniu wirusów, spyware'u i innych form złośliwego oprogramowania przy użyciu trzech komercyjnych silników skanujących oraz z wykorzystaniem sieci Websense ThreatSeeker Network, chroniąc w ten sposób sieć przed znanymi i nieznanymi zagrożeniami. Sieć ThreatSeeker zapewnia ochronę przed atakami typu zero-hour, nieustannie monitorując pocztę email oraz strony Web w celu wykrycia trendów oraz szablonów identyfikujących nowopowstające zagrożenia. Wyeliminowana zostaje w ten sposób luka w zabezpieczeniach pojawiająca się w czasie licznym od momentu pojawienia się nieznanego dotąd złośliwego kodu do chwili udostępnienia sygnatury umożliwiającej jego wykrycie. Usługa ta gwarantuje jakość na podstawie umowy SLA na poziomie 100 procent wykrywalności znanych wirusów.

Filtr zawartości

Zintegrowana technologia wiodących na rynku rozwiązań bezpieczeństwa danych firmy Websense, upraszcza zapobieganie utracie danych, spełnienie wymogów zgodności z obowiązującymi regulacjami oraz egzekwowanie polityk dopuszczalnego wykorzystania poczty. Predefiniowane słowniki pokrywające 20 tematów w 12 językach oraz wbudowane szablony standardów PCI-DSS i prywatności danych pomagają organizacjom w szybkiej identyfikacji i skutecznym powstrzymaniu aktów naruszenia polityk bezpiecznego korzystania z poczty email. Spełnienie specyficznych wymogów kontrolnych możliwe jest dzięki zastosowaniu wyrażen regularnych oraz elastycznych polityk. Akty naruszenia przyjętych norm identyfikowane są przy użyciu głębokiej analizy wiadomości email, jak również zawartości załączników. Wiadomości mogą być także kierowane do kwarantanny na podstawie faktycznego typu załączonego pliku lub dostarczane z opóźnieniem, jeśli przekraczają określony rozmiar.

Szyfrowanie

Szyfrowanie Websense zabezpiecza kanały komunikacji email, nie odbierając przy tym możliwości skanowania zaszyfrowanych wiadomości w poszukiwaniu złośliwego oprogramowania lub zawartości naruszającej polityki bezpieczeństwa. Websense obsługuje szyfrowanie typu server-to-server, korzystając ze standardu Transport Layer Security (TLS) oraz szyfrowania ad hoc typu park-and-pull dla komunikacji z klientami indywidualnymi. Polityki szyfrowania mogą być konfigurowane w oparciu o nadawcę, odbiorcę, ustawienia czułości Outlook lub słowo kluczowe w temacie wiadomości. Szyfrowanie może być łączone z filtrowaniem zawartości, w celu umożliwienia szyfrowania wiadomości email o określonej zawartości, takiej jak wrażliwe lub poufne informacje.

System usługi bezpieczeństwa Websense dla email pracuje równolegle z systemem usługi bezpieczeństwa Web firmy Websense, zapewniając zintegrowaną ochronę email i Web, umożliwiającą organizacjom skonsolidowanie zarządzania i raportowania dla obu usług.

Websense ThreatSeeker Network

Adaptacyjna technologia bezpieczeństwa ThreatSeeker Network korzysta z ponad 50 milionów działających w czasie rzeczywistym systemów gromadzenia danych, które nieustannie monitorują zawartość Internetu – w tym zawartość nowopowstałą oraz dynamiczną – zapewniając ochronę typu zero-hour przed pojawiającymi się atakami. Zgromadzona w ten sposób wiedza przekazywana jest w czasie rzeczywistym do systemów bezpieczeństwa Websense. Dzięki temu Websense jest w stanie dostosować się do gwałtownych zmian zachodzących w sieci Internet z prędkością nieosiągalną dla tradycyjnych rozwiązań bezpieczeństwa.

Cechy	Korzyści
Ochrona przed spamem i wirusami	Niezwykle precyzyjna (skuteczność gwarantowana umowami SLA) ochrona przed spamem, wirusami, spyware'em, phishingiem oraz zespolonymi zagrożeniami Web i email.
Wykrywanie zagrożeń typu zero-hour	System ochrony wspierany przez technologię ThreatSeeker Network identyfikuje i zatrzymuje nowopowstające zagrożenia eliminując podatność na nieznanne ataki.
Zapobieganie utracie danych	Zintegrowana technologia zaczerpnięta z wiodących na rynku rozwiązań bezpieczeństwa danych autorstwa Websense zapobiega ich utracie i pomaga spełnić wymogi zgodności z obowiązującymi regulacjami.
Filtrowanie zawartości	Predefiniowane słowniki zawartości pokrywające 20 tematów w 12 językach ułatwiają szybką identyfikację aktów naruszania polityk wykorzystania poczty email.
Szyfrowanie	Ochrona wrażliwych danych oraz danych objętych regulacjami przy użyciu technologii zabezpieczających kanały komunikacji z partnerami biznesowymi oraz osobami indywidualnymi.
Dostarczanie systemu w postaci usługi (Software-as-a-Service)	Oszczędność czasu i pieniędzy dzięki uniknięciu konieczności instalowania i utrzymywania dodatkowej infrastruktury, wbudowanej odporności, przewidywalnym kosztom oraz ograniczeniu ogólnych nakładów administracyjnych.
Wiodąca infrastruktura globalnych centrów danych	Dziesięć globalnych centrów danych o w pełni redundantnych systemach zasilania, chłodzenia i łączności z Internetem zapewnia wysoką dostępność oraz operatywność na poziomie 99.999 procent zgodnie z umowami SLA.
Certyfikacje bezpieczeństwa	Przyznanie ISO27001 jako rezultat niezależnych procedur certyfikujących i kontrolujących praktyki bezpieczeństwa zapewnia najwyższy poziom ochrony, prywatności i poufności.
Dostęp i wsparcie 24 godziny na dobę, 7 dni w tygodniu	Dostęp i zarządzanie usługą przez portal Web dostępny o każdej porze i z każdego miejsca. W razie potrzeby istnieje możliwość zwrócenia się o dodatkową pomoc (24 godziny na dobę, 7 dni w tygodniu).
Odzyskanie wiadomości w sytuacji awaryjnej	Wbudowana redundancja oraz <i>email spooling</i> zapobiegają nieodwracalnej utracie wiadomości email w przypadku pojawienia się awarii sieci lub serwera poczty.
Zarządzanie kwarantanną	Zaawansowany silnik wyszukiwania wiadomości zapewnia pełny wgląd i dostęp do logów oraz wiadomości umieszczonych w kwarantannie.
Samoobsługa użytkownika końcowego	Udzielanie użytkownikowi dostępu (zgodnie z harmonogramem lub na żądanie) do przeglądania i zwalniania wiadomości z kwarantanny, jak również do czarnych i białych list nadawców zmniejsza ogólne koszty administracyjne.
Integracja z usługami katalogowymi	Automatyczna synchronizacja adresów email i grup z Active Directory oraz LDAP upraszcza proces zarządzania polityką.
Administracja oparta na rolach	Kontrola dostępu osobno dla zarządzania kwarantanną, przeglądania raportów, dostępu do logów i innych kluczowych funkcji umożliwia delegowanie zadań administracyjnych.
Zapobieganie atakom „directory harvest”	Wbudowany system ochrony uniemożliwia spamującym gromadzenie prawidłowych adresów email.
Raportowanie	Ponad 40 różnych typów raportów, obejmujących zarówno raporty ogólne jak również szczegółowe analizy konkretnego elementu, zapewniają ogląd pełnej panoramy zagrożeń oraz ich ilości, jak również dostarczają informacje na temat przetworzonych wiadomości, aktów naruszania polityk bezpieczeństwa i wiele innych.

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

Zagrożenia w ruchu przychodzącym



- Spam
- Wirusy
- Złośliwe URLe

Zagrożenia w ruchu wychodzącym



- Wycieki danych
- Dozwolone użycie
- Zgodność

Wbudowane systemy ochrony Email i Web

- | | |
|---------------------|--------------------------------------|
| ✓ ThreatSeeker | ✓ Predefiniowane słowniki |
| ✓ Ochrona Zero-Hour | ✓ Głęboka analiza zawartości |
| ✓ Analiza URL | ✓ Zaawansowane dopasowywanie wzorców |

Inteligentne bezpieczeństwo email

Prywatność poczty elektronicznej

ISO 27001

System usługi bezpieczeństwa email firmy Websense został poddany niezależnemu audytowi i uzyskał certyfikację ISO 27001, co zapewnia najwyższy poziom bezpieczeństwa, prywatności i poufności. ISO 27001 jest normą standaryzującą system zarządzania bezpieczeństwem informacji (ISMS), opublikowaną w październiku 2005 przez Międzynarodową Organizację Normalizacyjną. Certyfikacja ta jest powszechnie uznawanym dowodem jakości programu bezpieczeństwa danej organizacji i uchodzi za najbardziej rygorystyczny standard bezpieczeństwa w branży, przewyższając wymagania normy SAS 70, którą szczyt się wiele firm konkurencyjnych.

Bezpieczeństwo centrów danych

Z wszystkich miejsc, do jakich trafić może Twoja poczta email, centra danych Websense są lokacjami najbezpieczniejszymi. Dzieje się tak dzięki zastosowaniu systemu zabezpieczeń i ochrony prywatności, który wbudowany jest bezpośrednio w sieć udostępniającą centrum danych. Czyste wiadomości, które nie zawierają podejrzanego kawałka kodu nie są zachowywane przez usługę, pozostałe wiadomości są widoczne jedynie dla użytkowników z uprawnieniami administracyjnymi oraz dla wszystkich tych, którym dostęp do konta został nadany. Centra danych Websense zachowują również najwyższe standardy ochrony przed dostępem fizycznym, takie jak:

- obsada personelem obsługującym centra 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku,
- systemy wykrywania fizycznej ingerencji,
- nadzór kamer przemysłowych,
- listy zastrzeżonego dostępu,
- fotograficzna i biometryczna weryfikacja pracowników.

Skrótowo o umowach dotyczących jakości świadczonych usług

Websense gwarantuje wiodące na rynku parametry SLA zapewniające najwyższy poziom świadczonych usług.

- **Dostępność** - 99,999 procent
- **Spam** – wykrywalność na poziomie co najmniej 99 procent
- **Wirusy** – 100- procentowa wykrywalność znanych wirusów
- **Opóźnienie przetwarzania** – maksymalnie 60 sekund dla wiadomości niesklasyfikowanych jako spam o rozmiarze poniżej dwóch megabajtów
- **Kwarantanna i logi** – dostępne po maksymalnie 5 minutach od chwili otrzymania wiadomości email

Wszystkie parametry SLA podlegają warunkom określonym w umowie o świadczenie usługi.



Aby dowiedzieć się więcej oraz przetestować rozwiązania Websense do ochrony poczty elektronicznej lub obejrzeć demo odwiedź www.websense.com/evaluations.