

Produkty		Moduły/Narzędzia	Właściwości	Zalety	
SZZEGÓŁY WEBSENSE KLIENT POLICY MANAGER I DODATKOWE MODUŁY – PATRZ DRUGA STRONA ULOTKI	Websense Enterprise®	Websense Enterprise	<p>Codziennie aktualizowana baza danych zawierająca ponad 22 miliony skategoryzowanych stron oraz 96 protokołów w ponad 50 językach.</p> <p>Zarządza dostępem do stron, które zmniejszają wydajność pracowników, np.: ogłoszenia, komunikatory, płatne serwisy, zakupy on-line oraz fora internetowe.</p> <p>Zarządza dostępem do stron wydatnie wpływających na zajętość pasma, np.: p2p, magazyny danych, radio i tv przez internet, telefonia internetowa.</p>	<p>Zarządzanie wykorzystaniem Internetu przez pracowników poprzez łatwy do obsługi interfejs.</p> <p>Zwiększenie wydajności pracowników poprzez zarządzanie dostępem do tych stron.</p> <p>Umożliwia właściwe wykorzystanie dostępnego pasma.</p>	
			Reporter	Raportowanie poprzez szczegółowe narzędzia analizy wyposażone w ponad 80 różnych szablonów raportów w wielu formatach, np.: PDF, Excel, itp.	Pomaga poznać sposób wykorzystania internetu w firmie i zweryfikować efektywność polityki jego wykorzystania. Dostępne są zarówno raporty graficzne jak i w postaci danych do analizy.
			Explorer	Wykorzystujące przeglądarkę narzędzie umożliwia ciągłe monitorowanie ruchu w sieci przez menedżerów działów informatyki, kadr i kierownictwa.	Szybki i łatwy dostęp do statystyk dotyczących działań pracowników, ich grup oraz całych działów.
		Real-Time Analyzer™	Graficzna reprezentacja ruchu sieciowego w czasie rzeczywistym uaktualniana domyślnie co 15 sekund.	Zapewnia ciągłą analizę najczęściej odwiedzanych stron WWW, najaktywniejszych pracowników oraz protokołów silnie obciążających pasmo.	
		Dynamic Protocol Management™	Umożliwia filtrowanie ruchu z uwzględnieniem ponad 96 protokołów podzielonych na ponad 15 kategorii.	Zarządzanie takimi protokołami jak P2P, media strumieniowe oraz komunikatory.	
		Dynamic Bandwidth Optimizer™	Redukuje i optymalizuje zasoby o dużych wymaganiach przepustowości pasma poprzez określanie priorytetów i zarządzanie ruchem sieciowym w czasie rzeczywistym.	Ograniczenie wykorzystania pasma przez mniej ważne aplikacje na rzecz priorytetowych aplikacji biznesowych.	
		WebCatcher™ & ProtocolCatcher™	Wylapuje niesklasyfikowane strony oraz protokoły i anonimowo przekazuje je do Websense celem klasyfikacji.	Niesklasyfikowane strony często odwiedzane przez pracowników podlegają dokładnemu zaszeregowaniu, Websense klasyfikuje strony.	
		File Type Manager	Pozwala pracownikom oglądać strony bez możliwości pobierania z nich określonych plików, np.: video, audio, wykonawczych, itp.	Zarządzanie przepustowością łącza i ochrona przed nieautoryzowanym pobieraniem danych.	
		Keyword Search, Cache & Proxy Avoidance	Umożliwia filtrowanie wyszukiwania informacji przez użytkowników przy użyciu słów kluczowych, a także filtrowanie zbuforowanych zawartości, stron tłumaczących, Akamai oraz mechanizmów wykorzystujących Proxy Avoidance.	Pozwala organizacjom egzekwować politykę korzystania z Internetu.	
		Search Filtering (SafeSearch)	Wymusza działania filtrów treści dla dorosłych w wiodących wyszukiwarkach.	Chroni przed oglądaniem stron www o potencjalnie obraźliwym charakterze.	
		Internet Watch Foundation Filtering	Pozwala zapobiegać dostępowi do witryn uznanych za nielegalne (np.: z dziecięcą pornografią, wulgarną zawartością).	Zapobiega dostępowi do stron z nielegalną zawartością.	
		Delegated Administration	Umożliwia zarządzanie polityką bezpieczeństwa w wielu oddziałach, organizacjach jak również zdalnymi serwerami poprzez funkcje centralnej dystrybucji konfiguracji.	Upraszcza kontrolę nad spójną polityką bezpieczeństwa, zwiększa elastyczność w dużych i rozproszonych organizacjach.	
		Delegated Reporting	Dostęp do narzędzi raportujących dla określonych użytkowników w celu oglądania raportów innych użytkowników lub grup.	Dostęp do kluczowych danych osobom upoważnionym (np. Marketing Manager może oglądać raporty dotyczące wyłącznie działu marketingu).	
		Auditing	Śledzenie i wgląd we wszystkie zmiany dokonywane w politykach Websense.	Umożliwia śledzenie zmian w konfiguracji polityk w celu rozwiązywania problemów i egzekwowania odpowiedzialności.	
		SNMP Alerting	Automatyczne wysyłanie powiadomień SNMP po przekroczeniu zdefiniowanych wartości progowych.	Możliwość integracji i wysyłania informacji do systemów zarządzania zdarzeniami bezpieczeństwa (SEM) oraz zarządzania tożsamością (IM).	
		Anonymous Logging	Opcja pozwalająca zachować anonimowość użytkowników podczas monitorowania ich aktywności.	Chroni prywatność użytkowników, zachowując szczegółowe informacje dotyczące zagrożeń wynikających z wykorzystania Internetu.	
		Selective Logging	Opcja umożliwiająca logowanie aktywności dla wybranych kategorii.	Redukuje koszt sprzętu poprzez wyeliminowanie gromadzenia informacji o nieistotnych kategoriach.	
		Security Filtering™	Websense skanuje ponad 600 milionów stron internetowych tygodniowo pod kątem złośliwego kodu, spyware, phishingu, potencjalnie niechcianego oprogramowania, które następnie są blokowane. Websense blokuje również wysyłanie poufnych informacji przez zainstalowane w systemie aplikacje spyware.	Chroni organizację i klientów przed złośliwym kodem, crimeware (tj. wirusy, konie trojańskie, robaki, keyloggers, itp.) jak również utratą poufnych danych oraz dostępem do nieuczciwych stron internetowych.	
	Malicious Traffic Management	Wykrywa, powiadamia i zapobiega generowaniu ruchu przez złośliwe aplikacje, takie jak boty, robaki mailowe, itp.	Wprowadza dodatkową warstwę zabezpieczającą przed coraz bardziej wymyślnymi aplikacjami crimeware oraz malware.		
	Websense Web Protection Services™	SiteWatcher™: Websense powiadamia klientów w przypadku zainfekowania stron domowych przez złośliwy kod mobilny lub spyware.	Ochrona przed zainfekowaniem komputerów organizacji oraz odwiedzających witrynę klientów i partnerów.		
BrandWatcher™: Websense powiadamia klientów w przypadku wykorzystania ich stron firmowych w atakach z użyciem phishingu lub keyloggerów.		Pozwala organizacjom na podjęcie szybkich kroków mających na celu ochronę ich klientów w przypadku skopiowania strony w nieuczciwych celach.			
ThreatWatcher™: Websense obserwuje serwer klienta www "okiem hakera" - regularnie skanuje znane podatności i potencjalne zagrożenia.		Szczegółowe raporty o poziomie zagrożenia i zalecanych działaniach w celu ochrony przed atakami.			
Real-Time Security Updates	Websense sprawdza dostępność aktualizacji nowych zagrożeń (złośliwy kod, spyware lub phishing) co 5 minut.	Sprowadza do minimum niebezpieczeństwo infekcji z nowo powstałych stron zawierających niebezpieczne komponenty.			
IM Attachment Manager™	Blokuje załączniki przesyłane za pomocą komunikatorów internetowych.	Umożliwia używanie komunikatorów bez ryzyka infekcji poprzez szkodliwe załączniki.			

Dodatkowe moduły do zestawów Websense Enterprise & Websense Security Suite

Dodatki	Moduły/Narzędzia	Właściwości	Zalety
Remote Filtering	Remote Filtering	Utrzymuje ochronę poprzez filtrowanie dostępu do internetu również dla pracowników mobilnych (bez konieczności zestawiania połączeń VPN).	Chroni mobilnych pracowników przed dostępem do stron zawierających złośliwy kod lub niewłaściwe treści oraz „wniesieniem” szkodliwego oprogramowania do sieci korporacji.
Websense Client Policy Manager™ (CPM)	Client Policy Manager	Określa jaki typ aplikacji może być uruchamiany na komputerach (stacje robocze, serwery, laptopy). Zapewnia bezpieczeństwo punktów końcowych z centralnej konsoli zarządzającej, wykorzystując codziennie aktualizowaną bazę zawierającą ponad 2.1 miliona aplikacji ujętych w ponad 50 kategoriach.	CPM kontroluje złośliwe i niechciane aplikacje. Pozostaje aktywny nawet w trybie offline. Wykrywa, analizuje i dostarcza proaktywną ochronę przed znanymi i nieznanymi zagrożeniami bezpieczeństwa.
	Remote Filtering	Utrzymuje ochronę poprzez filtrowanie dostępu do internetu również dla pracowników mobilnych (bez konieczności zestawiania połączeń VPN).	Chroni mobilnych pracowników przed dostępem do stron zawierających złośliwy kod lub niewłaściwe treści oraz „wniesieniem” szkodliwego oprogramowania do sieci korporacji.
	Removable Media Control	Zapobiega używaniu na komputerach PC urządzeń, takich jak pamięci flesz, nagrywarki CD/DVD, urządzenia zapisywalne, dyski zewnętrzne.	Zmniejsza ryzyko utraty bezpieczeństwa na skutek użycia przenośnych mediów.
	Application Control	Pozwala wykonać tylko zaakceptowane aplikacje.	Zwiększa bezpieczeństwo, uniemożliwiając uruchomienie potencjalnie niebezpiecznych aplikacji.
	Network Control	Blokuje dostęp aplikacjom sieciowym do wybranych portów i protokołów.	Zapobiega rozprzestrzenianiu się w sieci znanych i nieznanym zagrożeniom.
	Express Control	Natychmiast blokuje wykonanie nowych aplikacji.	Ochrona przed atakami keyloggerów „koni trojańskich”, robaków i innego szkodliwego oprogramowania.
	Microsoft® Windows XP Firewall Integration	Proste, ujednoczone zarządzanie i synchronizacja CPM z politykami Microsoft Firewall.	Pozwala wykorzystać ustawienia polityki Websense oraz wiedzę zawartą w bazie kategorii by dodać funkcje zarządzania i kontroli zawartości do usługi firewala.
	CPM Explorer	Wykorzystując przeglądarkę narzędzie umożliwia ciągłe monitorowanie wykorzystania aplikacji w ramach grup, wydziałów oraz użytkowników.	Szybki i łatwy dostęp do statystyk dotyczących wykorzystania aplikacji przez pracowników, ich grupy oraz całe działy.
	CPM Reporter	Raportowanie poprzez szczegółowe narzędzia analizy wyposażone w ponad 80 różnych szablonów raportów w wielu formatach, np.: PDF, Excel, itp., plus spis oprogramowania i sprzętu.	Dostarcza kompletny spis sprzętu i oprogramowania (aplikacje zainstalowane lub uruchamiane), co pozwala zweryfikować efektywność polityki ich wykorzystania. Dostępne są zarówno raporty graficzne jak i w postaci danych do analizy.
	AppCatcher™	Automatycznie i anonimowo przekazuje wszystkie nieznanne aplikacje do Websense celem klasyfikacji.	Niesklasyfikowane aplikacje uruchamiane przez pracowników podlegają dokładnemu zaszeregowaniu.

Websens ThreatSeeker™

Websense Web Security Suite wykorzystuje innowacyjną technologię Websense ThreatSeeker. Dostarcza ona wczesnej ochrony przed zagrożeniami bezpieczeństwa pochodzącymi z www, które zwykle są pomijane lub zapobieganie im z wykorzystaniem tradycyjnych technologii zabezpieczeń jest zbyt kosztowne. W przeciwieństwie do tych technologii Websense znajduje zagrożenia w internecie jeszcze zanim użytkownik będzie na nie narażony i długo przed opracowaniem łatek i sygnatur.

Websense ThreatSeeker używa ponad 100 własnych rozwiązań do rozpoznania złożonych zagrożeń dzięki wykorzystaniu algorytmów matematycznych, szablonów zachowań, analizy kodu, jak również rozległej sieci maszyn przetwarzających dane. Websense ThreatSeeker dostarcza rozległej wiedzy o zagrożeniach i automatycznej ochrony dla klientów w ciągu kilku minut.

Więcej informacji na temat Websense ThreatSeeker™ znajdziesz na: www.websense.com/threatseeker

© 2007 Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. v6.3 02/07

Dystrybucja w Polsce:



CLICO Sp. z o.o.
30-063 Kraków, Al. 3-go Maja 7
tel. 012 632-51-66
tel. 012 292-75-22 ... 25
fax 012 632-36-98
e-mail: support@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-555 Katowice, ul. Rolna 43
tel. 032 203-92-35
tel. 032 609-80-50
tel. 032 609-80-51
fax 032 203-92-24
e-mail: katowice@clico.pl

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

Websense
Anna Zawadzka
Territory Manager Poland
GSM +48 600 301512, fax +48 22 855 47 72
azawadzka@websense.com

© 2007 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.