WEBSENSE CLIENT POLICY MANAGER

Program Websense® Client Policy Manager™ (CPM) to wszechstronne rozwiązanie umożliwiające zabezpieczenie punktów końcowych dla komputerów stacjonarnych, przenośnych i serwerów do aktywnej ochrony organizacji przed znanymi i nieznanymi zagrożeniami bezpieczeństwa. Program CPM uniemożliwia instalowanie i uruchamianie nieautoryzowanych aplikacji oraz stosowanie zasad korzystania z aplikacji dzięki rozbudowanej, aktualizowanej codziennie bazie danych aplikacji podzielonych na kategorie. Program CPM to ważny element strategii zabezpieczeń punktów końcowych umożliwiający ochronę przed coraz bardziej zaawansowanymi i różnorodnymi zagrożeniami bezpieczeństwa.

„W przypadku komputerów przenośnych, na których obecnie zainstalowane jest oprogramowanie firmy Websense, od czasu wdrożenia nie wystąpiły żadne przypadki zarażenia wirusem ani instalacji oprogramowania typu spyware… otrzymaliśmy także pozytywne opinie od naszych użytkowników końcowych.”

Russell Ryan
Globalny administrator systemów Windows
Colorcon

ZADOWOLENI KLIENCI COLORCON

Problemy firmy Colorcon:

- Infekowanie komputerów przenośnych użytkowników zdalnych podczas ich pracy w terenie powodujące następnie wprowadzanie złośliwego oprogramowania do komputerów w organizacji.
- Infekcja robakiem NETSKY rozprzestrzeniająca się w sieci firmy Colorcon podczas trzygodzinnego etapu aktualizacji plików sygnatur programu antywirusowego.
- Pobieranie nieautoryzowanego oprogramowania, niezgodnego z oprogramowaniem biznesowym, co powoduje zwiększenie liczby połączeń z działem pomocy technicznej.

Korzyści w firmie Colorcon wynikające ze stosowania programu CPM:

- Baza danych aplikacji podzielonych na kategorie dostępna tylko w programie CPM umożliwia firmie Colorcon wygodne zarządzanie zasadami.
- Możliwość tworzenia niestandardowych zbiorów i kategorii reguł w programie CPM w celu tworzenia zasad dla „dozwolonych” aplikacji pozwala oszczędzić czas administracji.
- Łatwość użycia programu CPM pozwala na oszczędność czas i bezproblemową pracę działu IT.
- Dział pomocy technicznej firmy Colorcon może teraz działać zapobiegawczo, zamiast zajmować się nieoczekiwanymi problemami, których rozwiązanie wymaga dużych nakładów finansowych.

Zapobieganie atakom

Program CPM stanowi „pierwszą linię obrony” — ochrona zaczyna i kończy się w punkcie końcowym.

- Eliminacja słabych punktów używanych programów antywirusowych, programów do wykrywania oprogramowania typu spyware, zapór osobistych i procesów zarządzania instalowaniem poprawek w celu ochrony przed obecnie stosowanymi metodami ataku.
- Ochrona komputerów przenośnych pracujących poza siecią firmową lub tych, na których nie zainstalowano standardowych aktualizacji bądź poprawek bezpieczeństwa.
- Współpraca z rozwiązaniami z zakresu kontroli dostępu do sieci (NAC, Network Access Control) w celu stosowania zasad w przypadku urządzeń, które chcą uzyskać dostęp do sieci i blokowania niezgodnych urządzeń w punktach końcowych.
- Udostępnienie kilku poziomów kontroli w celu uniemożliwienia przeprowadzenia ataku lub powstrzymania kolejnych ataków związanych z zabezpieczeniami.

Websense Application Lockdown™ – zapewnia maksymalną kontrolę nad środowiskami komputerów stacjonarnych dzięki zezwalaniu na uruchomienie tylko zatwierdzonych aplikacji i uniemożliwianiu uruchomienia potencjalnie złośliwych aplikacji.

Websense Network Lockdown™ – blokuje dostęp aplikacji działającej w sieci do określonych portów i protokołów według kategorii aplikacji, co zapobiega rozprzestrzenianiu się złośliwego oprogramowania lub blokuje nieautoryzowany ruch wychodzący.

Websense Express Lockdown™ – umożliwia administratorom systemu zapobieganie atakom dzięki uniemożliwieniu uruchomienia złośliwego oprogramowania i ograniczeniu środowiska aplikacji do znanej konfiguracji.

Kontrola aplikacji używanych na komputerach stacjonarnych

Program CPM aktywnie monitoruje zainstalowane przez użytkownika aplikacje oraz ich działania i zmniejsza ilość połączeń z działem pomocy technicznej związanych z użyciem nieautoryzowanych aplikacji:

- Stosowanie uniwersalnych, automatycznie aktualizowanych zasad korzystania z aplikacji w celu ochrony użytkowników końcowych przed złośliwym oprogramowaniem.
- Zapobieganie instalacji i uruchamianiu nieautoryzowanych aplikacji.

Program CPM oferuje zaawansowane narzędzia do tworzenia raportów, które ułatwiają:

- Określ profil ryzyka Twojej organizacji.
- Wykrycie obecności i lokalizacji złośliwego kodu przenośnego (MMC, malicious mobile code), oprogramowania typu spyware, narzędzi stosowanych przez hakerów lub innych zagrożeń bezpieczeństwa na każdym komputerze i serwerze.
- Dokonaj ocen oprogramowania o znaczeniu krytycznym, które zapewniają uszeregowany według kategorii i znormalizowany przegląd programów i aplikacji.
- Wcześnie wykryj zagrożenia i zidentyfikuj potencjalne luki w zabezpieczeniach aplikacji.

Ochrona informacji

Program CPM stanowi kolejny poziom kontroli informacji na komputerach stacjonarnych dzięki uniemożliwieniu potencjalnej kradzieży poufnych informacji lub własności intelektualnej z wykorzystaniem nośników wymiennych lub przez sieć.

- **Websense Removable Media Lockdown**™ – pozwala administratorom systemów uniemożliwić korzystanie z urządzeń takich jak napędy flash, nagrywarki CD/DVD, stacje dyskietek i zewnętrzne dyski twarde na klienckich stacjach roboczych, co minimalizuje ryzyko wprowadzenia złośliwego oprogramowania do organizacji. W zależności zasad obowiązujących w organizacji można także uniemożliwić korzystanie z nośników zapisywalnych.

Uproszczone działanie

Program CPM pozwala na zmniejszenie nakładu pracy wymaganego do wdrożenia i zarządzania rozwiązaniami z zakresu zabezpieczeń dla punktów końcowych:

- Integracja z wiodącymi usługami katalogowymi.
- Udostępnienie zgodnego z systemem Microsoft Windows agenta, który ma niewielki wpływ na wydajność systemu.
- Optymalizacja działania działu IT i pomocy technicznej poprzez eliminację połączeń i interwencji związanych z ponowną instalacją systemu na komputerach stacjonarnych i przenośnych spowodowanych problemami z wydajnością lub zgodnością aplikacji.

Obsługa zaawansowanych technologii dostępnych tylko w produktach firmy Websense

Websense® Master Database – wykorzystuje kombinację opatentowanego oprogramowania do klasyfikacji i technik sprawdzania przez człowieka w celu zapewnienia jak największej skuteczności. Baza danych Websense Master Database zawiera najbardziej precyzyjną i aktualną klasyfikację adresów URL, protokołów i aplikacji.

- **Technologia Websense AppCatcher**™ – umożliwia klientom firmy Websense automatyczne i poufne przesyłanie nieznanych plików wykonywalnych w celu sprawdzenia i kategoryzacji. Firma Websense sprawdza elementy sieci i działanie aplikacji uruchamianych przez klientów, aby określić, czy zawierają złośliwy kod. Aplikacje są następnie dodawane do bazy danych, aby zapewnić ochronę wszystkim klientom.
- **Aktualizacje zabezpieczeń firmy Websense pobierane w czasie rzeczywistym** – zawierają aktualizacje bazy danych zabezpieczeń przed zagrożeniami związanymi z siecią Web i aplikacjami zaraz po wykryciu przez firmę Websense.

Filtrowanie dostępu do sieci Web dla użytkowników zdalnych

Funkcje zdalnego filtrowania w programie CPM umożliwiają zastosowanie tych samych zasad filtrowania dostępu do sieci Web dostępnych w produktach Websense Enterprise® lub Websense Web Security Suite™ również do użytkowników zdalnych i często podróżujących (jak gdyby pracowali oni w obrębie sieci), aby zapewnić pracownikom możliwość bezpiecznego korzystania z Internetu bez względu na miejsce pobytu.

- Rozszerzenie zasad korzystania z Internetu na zdalnych użytkowników komputerów przenośnych w celu ochrony ich przed złośliwymi i nieodpowiednimi witrynami sieci Web.

Wymagania systemowe

Serwer Client Policy Manager

- Microsoft Windows Server 2003 Standard Edition lub Enterprise Edition lub ten sam z dodatkiem SP1
- Microsoft Windows 2000 z dodatkiem SP3 lub nowszym

Klienty programów Client Policy Manager i Remote Filtering

- Microsoft Windows XP Professional z dodatkiem SP1 lub SP2
- Microsoft Windows Server 2003 Standard Edition lub Enterprise Edition z dodatkiem SP1
- Microsoft Windows 2000 Professional, Server lub Advanced Server z dodatkiem SP3 lub SP4

Serwer usługi Remote Filtering

- Microsoft Windows Server 2003 Standard Edition lub Enterprise Edition lub ten sam z dodatkiem SP1
- Microsoft Windows 2000 z dodatkiem SP3 lub nowszym
- Red Hat Enterprise Linux 3 lub 4: AS, ES lub WS, lub Red Hat Linux 9
- Sun Solaris 9 lub 10

Podsumowanie

Program CPM chroni komputery pracujące w sieci korporacyjnej i poza nią dzięki wykrywaniu i analizie zagrożeń bezpieczeństwa punktów końcowych i działań aplikacji oraz dzięki stosowaniu uniwersalnych, skalowalnych, automatycznie aktualizowanych zasad korzystania z aplikacji. Dzięki bezproblemowej integracji z istniejącą infrastrukturą IT, program CPM chroni wszystkich użytkowników przed znanymi i nieznanymi zagrożeniami bezpieczeństwa.

Websense, Inc.
San Diego, CA USA
tel. +1 858 320 8000
fak s +1 858 458 2950
www.websense.com

Websense UK Ltd.
Chertsey, Surrey UK
tel. +44 (0) 1932 796300
fak s +44 (0) 1932 796601
www.websense.co.uk

Australia
websense.com.au

Brazylia
portugues.websense.com

Francja
websense.fr

Hiszpania
websense.com.es

Hong Kong
websense.cn

Indie
websense.com

Irlandia
websense.ie

Japonia
websense.jp

Kolumbia
websense.com.es

Meksyk
websense.com.es

Niemcy
websense.de

PRC
prc.websense.com

Tajwan
websense.cn

Włochy
websense.it

Aby uzyskać informacje o punktach sprzedaży produktów firmy Websense, przejdź do witryny www.websense.com/partner_europe

Pobierz darmową, 30dniową wersję testową już dzisiaj www.websense.com/downloads

WEBSENSE
SECURING PRODUCTIVITY™