

## McAfee Enterecept Web Server Edition

### Sprawdzona ochrona serwerów WWW przed włamaniami

#### Wyzwanie

Skuteczna ochrona serwerów WWW jest trudnym wyzwaniem. Ponieważ serwery WWW z definicji muszą być dostępne z zewnątrz, znajdują się w zasięgu napastników z całego świata. Ponadto w sieciach WWW wykryto setki luk w zabezpieczeniach, co czyni z nich łatwy cel ataków. Podmienianie stron internetowych staje się coraz częściej metodą zwrócenia na siebie uwagi, stosowaną przez organizacje wywrotowe i napastników.

Zapory i zabezpieczenia graniczne nie sprawdzają się już w przedsiębiorstwach jako skuteczne środki ochrony. Hakerzy mają na tyle dużą wiedzę, że odkrywają sposoby obejścia zapór i istniejących systemów wykrywania, aby podczas ataku wykorzystywać na przykład przepełnienia buforu czy robaki bezpośrednio skierowane przeciw serwerom i aplikacjom. Na przykład wirus Code Red przedostał się przez zapory i sieciowe systemy IDS, wyrządzając olbrzymie szkody. Specjaliści szacują spowodowane przez niego straty gospodarcze na 2,62 mld USD. Serwery WWW potrzebują dzisiaj lepszej ochrony przed coraz bardziej zróżnicowanymi zagrożeniami: podmianami stron internetowych, przepełnianiem buforów, robakami, nowo odkrytymi atakami itp. Nasilone środki bezpieczeństwa są niezbędne, aby chronić serwery WWW przed atakami zarówno dziś, jak i w przyszłości.

#### Rozwiązanie McAfee Enterecept Web Server Edition

McAfee® Enterecept® Web Server Edition (WSE) rozpoznaje ataki i zapobiega nieautoryzowanemu dostępowi do zasobów serwera WWW, zanim dojdzie do jakichkolwiek bezprawnych transakcji. Wykorzystując funkcje oprogramowania Enterecept Standard Edition, wersja Web Server Edition zapobiegawczo chroni host, ponieważ ocenia żądania kierowane do serwera WWW, interfejsu programowania aplikacji (API) oraz systemu operacyjnego, zanim zostaną one przetworzone. Oprogramowanie Enterecept chroni zarówno system operacyjny, jak i aplikacje, co pozwala uniknąć niepożądanych skutków znanych i nieznanymi ataków.

#### Korzyści, jakie daje McAfee Enterecept Web Server Edition

##### Mniej przestojów

- Uniemożliwia podmienianie stron internetowych.
- Zapobiega włamaniam do serwera.
- Chroni przed wykorzystywaniem przepełnienia buforu.

##### Niższe koszty związane z bezpieczeństwem

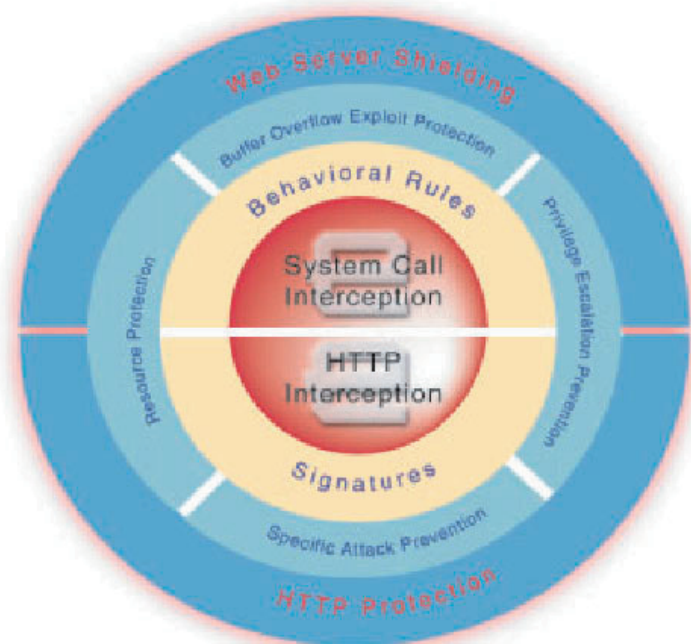
- Znacznie ogranicza koszty odtwarzania związane z przestojem.
- Zmniejsza zapotrzebowanie na wyspecjalizowany personel.

##### Ochrona majątku

- Chroni dane klientów.
- Uniemożliwia napastnikom rozpoczęcie ataków na inne serwery z serwera WWW.

##### Ochrona reputacji

- Uniemożliwia podmienianie stron internetowych.



**Wielopoziomowe rozwiązanie McAfee Enterecept skutecznie chroni serwery WWW o znaczeniu krytycznym.**

#### Jak działa Enterecept WSE

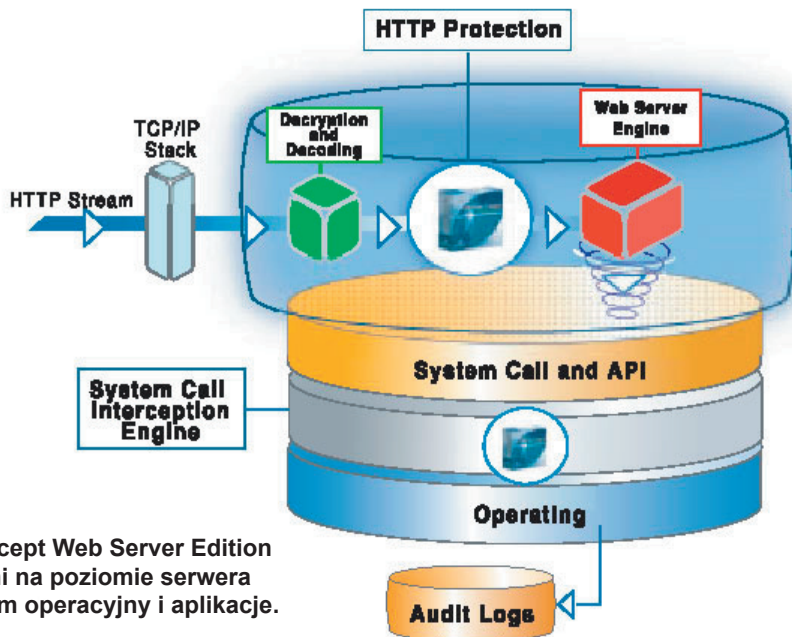
Program Enterecept chroni serwery korporacyjne przy wykorzystaniu różnych technologii. Rozproszona architektura umożliwia zainstalowanie agenta Enterecept na każdym serwerze w przedsiębiorstwie. Agenty Enterecept przechwytyją wywołania wysyłane do systemu operacyjnego i blokują te, które mogą być szkodliwe. Enterecept określa m.in. proces źródłowy wywołania, użytkownika, który wysłał wywołanie, zasoby, na których operuje wywołanie, oraz uprawnienia użytkownika związane z wywołaniem. Na podstawie tych informacji wywołania są porównywane z odpowiednimi modelami zachowania i sygnaturami znanych ataków. Następnie Enterecept blokuje wywołania próbujące wyrządzić jakies szkody lub odpowiadające określonej sygnaturze ataku. Wszystkie działania zapobiegawcze są rejestrowane w Enterecept Management System, co umożliwia ich przeglądanie i tworzenie raportów.

W dołączonej do produktu bazie danych zasad znajduje się w pełni skonfigurowany szablon domyślny z funkcjami dostosowywania, co pozwala na niemal całkowite wyeliminowanie fałszywych trafień. Domyślne zasady zapewniają ponadto szybkie wdrażanie. Agenty zainstalowane na każdym komputerze biurowym są kontrolowane i aktualizowane przez Enterecept Management System.

Agenty są samowystarczalnymi jednostkami ochronnymi i ich funkcjonowanie nie jest uzależnione od systemu zarządzania. Sprzyja to zarówno niezawodności, jak i większemu bezpieczeństwu. Agenty pobierają aktualizacje, w tym aktualizacje kodu i nowe definicje ataków, z systemu zarządzania. Cała komunikacja odbywa się za pośrednictwem szyfrowania RC4 i protokołu wymiany kluczy Diffie-Hellman.

# McAfee Enterccept Web Server Edition

## Sprawdzona ochrona serwerów WWW przed włamaniami



Enterccept Web Server Edition chroni na poziomie serwera system operacyjny i aplikacje.

**Ochrona serwera WWW** — Ochrona serwera WWW tworzy tarczę ochronną wokół serwerów WWW Apache, iPlanet oraz Microsoft IIS. Chroni w ten sposób aplikację serwera WWW wraz z jej zasobami, czyli również danymi. Ochrona zostaje zainstalowana po określeniu konfiguracji serwera przez adaptacyjny proces audytu. Od tego momentu chroni ona serwer WWW zarówno przed penetracją z zewnątrz, jak i przed szkodliwym nadużyciem. Dzięki temu znane i nieznane ataki są na bieżąco odpierane, zanim zdołają dotrzeć do serwera i wyrządzić szkody. Potencjalni intruzi nie mogą podmienić stron internetowych ani zmodyfikować parametrów operacyjnych — nawet jeśli uzyskają uprzywilejowany dostęp do serwera.

**Ochrona HTTP** — Ochrona HTTP, przy użyciu żądań HTTP, blokuje ataki na serwery WWW Apache, iPlanet oraz Microsoft IIS Web. Proces analityczny sprawdza strumień HTTP, identyfikuje

szkodliwe żądania i uniemożliwia im dotarcie do serwera WWW, zanim wyrządzą one szkody. Technologia ta chroni przed popularnymi sposobami atakami na serwery WWW, takimi jak zdalne wykonywanie kodu, podmiana ścieżek (directory traversal) i ujawnianie pliku. Jest skuteczna nawet wtedy, gdy intruzi próbują uniknąć wykrycia przez szyfrowanie na poziomie aplikacji, na przykład SSL, powszechnie stosowane w serwisach internetowych handlu elektronicznego. Pełną ochronę aplikacji uzyskuje się dopiero w połączeniu z innymi metodami obrony Enterccept.

**Wszystkie funkcje Enterccept Standard Edition** — Enterccept Web Server Edition zawiera, oprócz wyżej opisanych, wszystkie funkcje oferowane przez Enterccept Standard Edition, takie jak ochrona przed znanymi i nieznanymi atakami, zapobieganie wykorzystywaniu przepełnienia buforu, ochrona zasobów, ochrona przed podniesieniem uprawnień oraz SecureSelect.

### Właściwości

- wyjątkowa osłona gwarantująca całkowitą ochronę serwera WWW
- zapobiegawcza reakcja na atak, umożliwiająca zakończenie lub zamknięcie procesu przed powstaniem szkód
- brak potrzeby stałego monitorowania zabezpieczeń
- bezpieczne, samowystarczalne agenty
- fabrycznie skonfigurowany szablon zasad ze wszystkimi opcjami dostosowywania
- zapobieganie szkodliwemu dostępowi do zasobów systemu
- uzupełnienie dotychczasowej infrastruktury zabezpieczeń bez konieczności integracji.

### Wymagania instalacyjne

#### Serwer WWW Windows

- IIS 4
- IIS 5

#### Serwer WWW Solaris

- Apache 1.3.6 i nowszy
- Apache 2.0.42 i nowszy
- iPlanet 4.0 i 4.1
- SunOne 6.0

Wszystkie produkty Network Associates® są obsługiwane przez program PrimeSupport® i Network Associates Laboratories. W ramach dostosowanej usługi PrimeSupport dostarczane są ogólne informacje o produktach i szybkie, niezawodne rozwiązania techniczne zapewniające niezawodne i nieprzerwane działanie. Stały rozwój i doskonalenie naszych technologii gwarantuje Network Associates Laboratories — światowy lider bezpieczeństwa i systemów informacyjnych.