

McAfee Enterecept Standard Edition

System zapobiegania włamaniom do serwerów korporacyjnych

Wyzwanie

Ochrona przedsiębiorstwa to zadanie, które z każdym dniem staje się coraz trudniejsze. Zespół CERT (Computer Emergency Response Team) informuje, że co roku liczba zgłoszonych prób naruszenia bezpieczeństwa podwaja się. W bieżącym roku stwierdzono niemal dwa razy więcej luk w zabezpieczeniach, niż w roku ubiegłym. Nieustanne wykorzystywanie najnowszych technik przez włamywaczy czyni ich ataki coraz trudniejszymi do powstrzymania. Zapory i narzędzia ochrony brzegowej nie wystarczają już do ochrony przedsiębiorstwa. Dysponujący coraz większą wiedzą hakerzy znaleźli sposoby na ominięcie zapór i innych dotychczasowych systemów wykrywania włamań, i za pomocą takich technik, jak przepełnienie bufora czy robaki internetowe atakują bezpośrednio serwery i aplikacje. Robak o nazwie Code Red skutecznie ominął zapory i systemy wykrywania włamań, wywołując ogromne szkody. Firma Computer Economics ocenia, że globalne straty wywołane przez robaka Code Red wyniosły 2,62 mld USD. Potrzeba zastosowania lepszego systemu zabezpieczeń wynika m.in. z następujących okoliczności:

- gwałtownie rosnąca liczba luk w zabezpieczeniach
- rozwój technik ataków
- niezdolność dotychczasowych rozwiązań do ochrony przed nowymi zagrożeniami.

System Enterecept

System McAfee® Enterecept® odpowiada zarówno obecnym, jak i przyszłym potrzebom przedsiębiorstw związanych z ochroną serwerów, zabezpieczając je przed znanymi i nieznanymi formami ataków. Oparty na opatentowanej technologii system Enterecept ogranicza czas przestoju, redukuje koszty związane z bezpieczeństwem i chroni krytyczne zasoby przedsiębiorstwa. Rozwiązanie wykorzystuje ochronę prewencyjną, analizując wywołania kierowane do systemu operacyjnego, zanim zostaną one wykonane. W odróżnieniu od innych rozwiązań zabezpieczających, system Enterecept stosuje połączenie reguł zachowań i sygnatur, dzięki czemu jest w stanie zapobiegać znanym i nieznanym atakom i nie ogranicza się tylko do wykrywania ataków i informowania o nich użytkownika. Enterecept to sprawdzony lider na rynku systemów zapobiegania włamaniom.

Korzyści

Krótszy czas przestoju

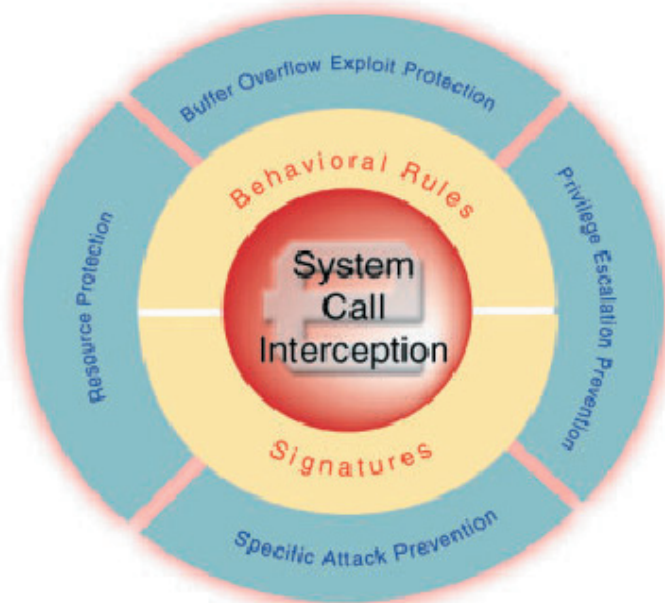
- Zapobiega atakom, nie ograniczając się jedynie do ich wykrywania.
- Chroni przed atakami wykorzystującymi przepełnienie bufora.

Niższe koszty związane z bezpieczeństwem

- Minimalizuje koszty odtwarzania wynikające z przestoju.
- Ogranicza konieczność angażowania specjalistów.

Ochrona zasobów

- Chroni dane klientów.
- Osłania aplikacje.
- Strzeże renomy przedsiębiorstwa.



Funkcja przechwytywania wywołań udostępniana przez system McAfee Enterecept wykorzystuje sygnatury i reguły zachowań do zapobiegania przepełnieniu buforów lub uzyskaniu nadmiernych uprawnień, a także ochrony przed innymi, znanymi i nieznanymi formami ataków.

Jak działa system Enterecept?

System Enterecept łączy w sobie kilka kluczowych technologii ochrony serwerów korporacyjnych. Na każdym serwerze przedsiębiorstwa, w ramach architektury rozproszonej, instalowane są Agenty Enterecept. Przechwytyują one wywołania kierowane do systemu operacyjnego, blokując te spośród nich, które mogą przynieść destrukcyjne skutki. System określa m.in. proces wysyłający wywołanie, użytkownika wysyłającego wywołanie, zasób będący przedmiotem wywołania oraz uprawnienia użytkownika związane z wywołaniem. Dzięki tym informacjom wywołania zostają dopasowane do odpowiednich reguł zachowań i sygnatur znanych ataków.

Następnie system blokuje zapytania związane z destrukcyjnym zachowaniem lub takie, które pasują do jednej z sygnatur. Wszelkie działania prewencyjne są rejestrowane w systemie Enterprise Management System, a następnie udostępniane do wglądu i uwzględniane w raportach.

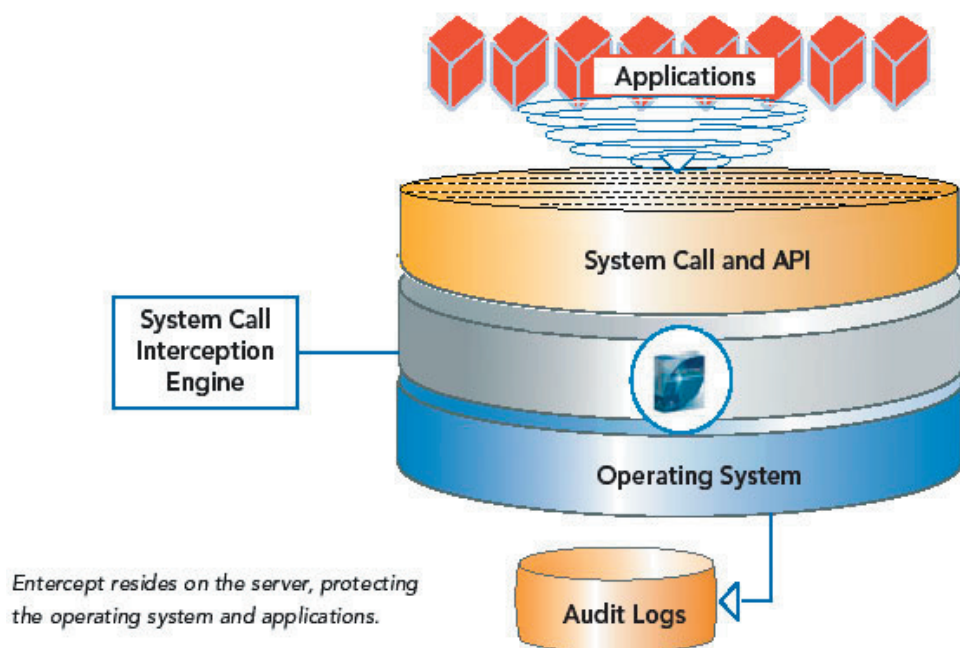
Baza danych reguł zawiera w pełni skonfigurowany szablon domyślny, wyposażony w rozbudowane funkcje dostosowywania ustawień, co pozwala na niemal całkowitą eliminację fałszywych alarmów. Użycie reguł domyślnych umożliwia szybkie wdrożenie.

Agenty są wdrażane na każdym serwerze z osobna, a ich kontrolowanie i aktualizacja odbywają się za pośrednictwem systemu Enterecept Management System. Agenty stanowią całkowicie autonomiczne jednostki ochronne, które mogą funkcjonować niezależnie od systemu zarządzania. Do zalet takiego rozwiązania należy większa niezawodność i wyższy poziom bezpieczeństwa.

Agenty pobierają z systemu zarządzania aktualizacje, np. nowe wersje kodu programu czy nowe definicje ataków. Komunikacja między agentami a systemem odbywa się z użyciem szyfrowania RC4 i algorytmu wymiany kluczy Diffiego-Hellmana.

McAfee Intercept Standard Edition

System zapobiegania włamaniom do serwerów korporacyjnych



Ochrona zasobów — Blokując zasoby systemowe o krytycznym znaczeniu (newralgiczne pliki, ustawienia, klucze rejestru, usługi itp.), Intercept chroni systemy przed niepowołanym dostępem.

Ochrona przed uzyskaniem nadmiernych uprawnień — Sposób działania wielu włamywaczy zakłada uzyskanie dostępu do konta o niskich uprawnieniach, a następnie wykorzystanie luk w zabezpieczeniach w celu uzyskania uprawnień administratora. System Intercept blokuje takie ataki i uniemożliwia zwiększenie uprawnień przez włamywaczy.

Funkcja SecureSelect™ — System Intercept udostępnia trzy tryby zabezpieczeń: ostrzegawczy (SecureSelect Warning Mode), ochronny (SecureSelect Protection Mode) i skarbcza (SecureSelect Vault Mode). Każdy kolejny tryb zapewnia wyższy poziom bezpieczeństwa. Klienci rozpoczynają wdrożenie systemu od trybu ostrzegawczego, a następnie, w miarę dostrajania i dopracowywania funkcji bezpieczeństwa, uaktywniają tryb ochronny i tryb skarbcza.

Funkcje

- Funkcja zapobiegania atakom umożliwia blokowanie

destrukcyjnych działań, zanim doprowadzą one do powstania szkód.

- Bezpieczne, samodzielne agenty.
- Wstępnie skonfigurowany szablon reguł wyposażony w pełne opcje dostosowywania.
- Zapobieganie dostępowi bez upoważnienia do zasobów systemowych.
- Uzupełnienie istniejącej infrastruktury bezpieczeństwa.

Wymagania systemowe

Agent—Windows

- Windows® 2000 Server lub Advanced Server
- Windows NT 4 Server lub Enterprise Server, Service Pack 4 lub nowszy

Agent—Solaris

- Solaris 2.6 (jądro 32-bitowe)
- Solaris 8 (32-bit and 64-bit kernel)
- Solaris 7 (jądro 32-bitowe i 64-bitowe)
- Solaris 9 (32-bit and 64-bit kernel)

Agent—HP-UX

- HP-UX 11i (64-bit PA-RISC)
- HP-UX 11.0 (64-bit PA-RISC)

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.

networkassociates.com



YOUR NETWORK. OUR BUSINESS.™