



## McAfee Enterccept Desktop Agent

Ochrona notebooków i komputerów biurkowych przed włamaniami

### Wyzwanie

Konwencjonalne programy antywirusowe nie zapewniają użytkownikom notebooków i komputerów biurkowych wymaganego poziomu dostępności, integralności i poufności. Systemy te zawierają te same zastrzeżone i chronione przepisami dane, które znajdują się na serwerach korporacyjnych, ale nie są objęte ochroną zabezpieczeń firmowych, takich jak zapory sieciowe i systemy zapobiegające włamaniom do sieci. Bezpieczeństwo przechowywanych w nich danych jest więc zagrożone.

Przedsiębiorstwa powinny chronić systemy najbardziej podatne na zagrożenia za pomocą zaawansowanych rozwiązań do ochrony prewencyjnej, zabezpieczających przed atakami wykorzystującymi luki w zabezpieczeniach. Konwencjonalne programy antywirusowe działają w sposób interwencyjny i nie blokują ataków nieznanymi (klasy „zero-day”), wykorzystujących nowo odkryte luki w zabezpieczeniach. Ponadto wszystkie firmy, niezależnie od wielkości, muszą przestrzegać przepisów mówiących o konieczności ochrony poufnych danych i kontrolowania dostępu do systemów i aplikacji.

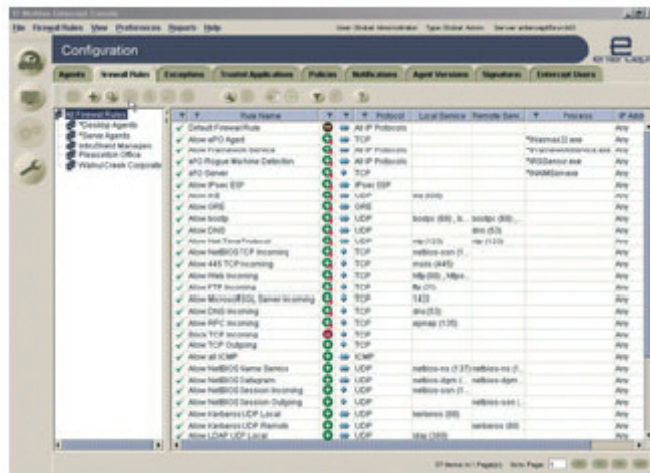
Aby zagwarantować kompleksową, prewencyjną ochronę komputerów przenośnych i biurkowych przed włamaniami, przedsiębiorstwa i instytucje powinny wdrożyć systemy zabezpieczające klasy korporacyjnej. System McAfee® Enterccept® zapewnia najdokładniejszą i najbardziej rozszerzalną ochronę przed włamaniami do komputerów biurkowych i przenośnych ze wszystkich rozwiązań dostępnych obecnie na rynku. Pozwala przedsiębiorstwom zmniejszyć ryzyko, zapewnić ciągłość działania i obniżyć całkowity koszt posiadania.

### Rozwiązanie McAfee Enterccept do notebooków i komputerów biurkowych

Agenty systemu McAfee Enterccept chronią komputery przenośne i biurkowe zarówno przed atakami nieznanymi (klasy „zero day”), jak i przed zagrożeniami znanymi, wykorzystując tę sama opatentowaną technologię, której używają agenty systemu Enterccept do serwerów. Agenty Enterccept Desktop zawierają reguły zachowań sformułowane na potrzeby ochrony przed zagrożeniami klasy „zero-day”, bez korzystania z uaktualnień, najczęściej atakowanych aplikacji komputerów biurkowych, takich jak Microsoft® Internet Explorer i Outlook.

Każdy z tych centralnie zarządzanych agentów wykorzystuje unikatowy zestaw trzech technologii ochrony przed włamaniami, za pomocą których skutecznie blokuje ataki na usługi i aplikacje używane na komputerach osobistych.

- Reguły zachowań chronią przed atakami klasy „zero-day” wykorzystującymi nowo wykryte luki w zabezpieczeniach oraz luki, do których nie ma programów korygujących tzw. poprawek. Dzięki temu wdrażanie programu korygującego nie jest tak pilne.
- Sygnatury służą do zabezpieczenia hostów, dokładnie identyfikując znane zagrożenia zawarte w danych i blokując niebezpieczne ładunki przed ich przetworzeniem, co znacznie zmniejsza liczbę przypadków błędnego rozpoznania zagrożeń.



System Enterccept jest niewidoczny dla użytkownika, a szczegółowymi, dostosowywanymi regułami zarządza administrator.

- Zapora systemowa zabezpiecza aplikacje i dane, blokując ruch przychodzący i wychodzący na podstawie kontroli adresu IP, protokołu lub portu.

### Korzyści

#### Kompleksowa ochrona

- Blokuje ataki klasy „zero-day” bez uaktualnień.
- Znacznie zmniejsza potrzebę szybkiego wdrażania programów korygujących w przypadku wykrycia nowych zagrożeń.
- Zapewnia dostępność, integralność oraz poufność danych i systemów.
- Mechanizm zapobiegania włamaniom i zapora zabezpieczają przed atakami komputery biurkowe i przenośne.

#### Dokładność

- Definiując „zaufane oprogramowanie”, firmy unikają błędnego rozpoznawania zagrożeń w aplikacjach o znaczeniu krytycznym.
- Sygnatury znacznie zmniejszają liczbę przypadków błędnego rozpoznawania zagrożeń oraz umożliwiają szczegółowe opisanie zdarzeń.
- Dostosowywane reguły zapewniają zgodność z każdym środowiskiem.

#### Rozszerzalność

- Jeden system umożliwia zarządzanie nawet 10 tys. agentów.
- Możliwość opcjonalnego zarządzania za pomocą programu McAfee ePolicy Orchestrator® 3.x.
- Niewidoczna instalacja i uaktualnianie bez restartu systemu lub udziału użytkownika zapobiegają naruszaniu reguł.
- Automatyczne reagowanie na zdarzenia związane z bezpieczeństwem i brak lokalnego interfejsu użytkownika zapobiegają przypadkowemu naruszeniu bezpieczeństwa przez użytkowników.



## Jak działa system McAfee Enterecept

Każdy agent systemu Enterecept ma w pełni skonfigurowane domyślne szablony reguł ochrony, co zapewnia bezpieczeństwo od razu po uruchomieniu systemu. Ponadto agenty mają rozbudowane funkcje konfiguracyjne, które umożliwiają specjalistom w dziedzinie zabezpieczeń tworzenie i dostrajanie reguł odpowiadających wymaganiom konkretnego środowiska. Zmniejsza to liczbę przypadków błędnego rozpoznania zagrożeń.

Agent bada określone odwołania do systemu operacyjnego i interfejsu programowania API (wykorzystywane przez wszystkie aplikacje do zgłaszania żądań obsługi do systemu operacyjnego). Szybko i efektywnie porównuje swoje reguły zachowań i sygnatury znanych ataków z informacjami o każdym odwołaniu (takimi jak proces zgłaszający odwołanie, kontekst zabezpieczeń tego procesu, zasoby, do których żąda dostępu, itd.) Następnie agent blokuje wszystkie odwołania związane z podejrzanym zachowaniem lub szkodliwym kodem.

Agenty automatycznie wyszukują w systemie zarządzania zaszyfrowane i uwierzytelnione uaktualnienia, dzięki czemu zawsze zawierają najnowsze reguły i sygnatury ataków.



*Enterecept zapewnia dostępność, integralność i poufność danych w notebookach i komputerach biurowych.*

### Najważniejsze funkcje

Zapobieganie atakom nieznanym (klasy „zero-day”) — Enterecept zapobiega nowym, wcześniej nieznanym atakom wykorzystując efektywne reguły zachowań, niewymagające uaktualnień. Takie podejście pozwala egzekwować prawidłowe zachowanie systemu operacyjnego i aplikacji oraz blokować nowe ataki naruszające reguły.

Zapobieganie przepełnieniu bufora — Opatentowana technologia uniemożliwiająca wykonanie kodu w wyniku przepełnienia bufora, które jest najczęstszym źródłem podatności systemu na zagrożenia.

Zapobieganie znanym atakom — Wykrywa i blokuje znane zagrożenia oraz zapobiega powstaniu szkód w systemie, porównując jego aktywność z informacjami o znanych atakach

pochodzącymi z obszernej, automatycznie uaktualnianej bazy danych; ponadto sporządza szczegółową ekspertyzę.

Zapora systemowa — Blokuje ruch przychodzący i wychodzący za pomocą bardzo dokładnego filtra pakietów oraz zapytań. Blokowanie może następować na podstawie analizy portów, protokołów i adresu IP.

Ochrona zasobów — Zabezpiecza system przed zagrożeniami, blokując dostęp do najważniejszych zasobów (plików, ustawień, kluczy rejestru, usług itd.). Uniemożliwia obejście reguł bezpieczeństwa nawet użytkownikom z uprawnieniami administratora.

Niewidoczność dla użytkowników — Agenty są niewidoczne dla użytkownika i nie wymagają jego udziału w instalacji, uaktualnianiu i reagowaniu na zagrożenia bezpieczeństwa.

Lokalna kontrola dostępu — Blokuje dostęp do dysków pamięci masowej USB, napędów dyskietek itd.

Ochrona aplikacji osłonami i otoczkami — Technologia ta zapobiega penetracji z zewnątrz i niewłaściwemu wykorzystaniu zasobów programów Internet Explorer i Microsoft Outlook (plików, użytkowników, rejestru itd.). Otoczka uniemożliwia tym aplikacjom szkodliwą aktywność, wykraczającą poza normalne zachowanie (np. dostęp do danych innych aplikacji).

Szybkie wdrażanie reguł bezpieczeństwa w konfiguracji standardowej — Intuicyjna w obsłudze konsola zarządzania umożliwia stopniowe zwiększanie poziomu czułości agentów i własnego bezpieczeństwa. W rezultacie można niemal wyeliminować przypadki błędnego rozpoznawania zagrożeń i ograniczyć potrzebę długoterminowego dostrajania.

Scentralizowane zarządzanie — System zarządzania pozwala przedsiębiorstwu egzekwować konfigurowanie i przestrzeganie reguł bezpieczeństwa we wszystkich aplikacjach, grupach użytkowników i agentach, co zmniejsza koszty instalacji i konserwacji.

### Wymagania systemowe

**Windows (tylko wersje angielska, francuska i niemiecka)  
Wersja na Polskie systemy operacyjne dostępna od 2006r.**

- Windows XP SP2, Windows 2000 Workstation lub Windows NT 4 Workstation

### McAfee PrimeSupport

Program McAfee PrimeSupport® jest elementem niezbędnym do maksymalnego wykorzystania inwestycji w rozwiązania do ochrony systemów i sieci firmy McAfee. Zespół PrimeSupport dysponuje wszelkimi niezbędnymi zasobami i jest gotowy do świadczenia usług wymaganych przez klienta. W ramach programu PrimeSupport można korzystać m.in. z dostępu do wszystkich wersji serwisowych i uaktualnień produktów oraz do kompleksowego zestawu dodatkowych internetowych mechanizmów samopomocy, telefonicznej pomocy technicznej dostępnej przez 24 godziny na dobę i 7 dni w tygodniu, pomocy wyznaczonych opiekunów klienta ds. pomocy technicznej oraz szeregu innych usług pomocy technicznej w zakresie sprzętu i oprogramowania, które można dostosować do potrzeb klienta.