

wirusy ✓  
spyware ✓  
adware ✓  
phishing ✓

## NOD32 for MS Exchange Server

Nowoczesny program antywirusowy przeznaczony do ochrony poczty elektronicznej i folderów publicznych serwerów MS Exchange. Program NOD32 for MS Exchange Server wykrywa w czasie rzeczywistym wszystkie rodzaje wirusów, robaków i programów adware i spyware, które infekują system za pośrednictwem poczty. Unikalna technologia ThreatSense™ łącząca metodę zaawansowanej analizy heurystycznej ze skanowaniem na podstawie bazy sygnatur zapewnia skuteczną ochronę również przed nowymi, jeszcze niesklasyfikowanymi zagrożeniami.

### Najważniejsze funkcje:

- ▶ Pełna ochrona poczty przychodzącej i wychodzącej przed wirusami, programami spyware, adware i próbami phishingu.
- ▶ Unikalna technologia ThreatSense™ wykrywająca nowe zagrożenia od momentu ich pojawienia się, jeszcze przed aktualizacją bazy sygnatur.
- ▶ Skanowanie na żądanie zasobów serwera MS Exchange.
- ▶ Ochrona folderów publicznych w czasie rzeczywistym.
- ▶ Pełna ochrona serwera, na którym działa system MS Exchange.
- ▶ Definiowanie reguł dotyczących skanowania i postępowania z zainfekowanymi wiadomościami.
- ▶ Automatyczna, inkrementacyjna aktualizacja bazy sygnatur nawet co godzinę.
- ▶ Skanowanie zabezpieczonych hasłem dokumentów MS Office, plików skompresowanych i chronionych plików wykonywalnych.
- ▶ Filtrowanie wiadomości według tematu, nadawcy lub nazwy załącznika umożliwiające zablokowanie wybranych przesyłek.
- ▶ Przejrzysty dziennik zdarzeń z kompletną informacją na temat dokonanych aktualizacji, wyników skanowania i wykrytych infekcji.

wirusy ✓  
spyware ✓  
adware ✓  
phishing ✓

### Technologia ThreatSense™

ThreatSense™ jest nową, stworzoną przez firmę ESET, technologią wykrywania wirusów i innych wrogich programów takich jak robaki komputerowe, spyware, adware i wiele innych. Łączy w sobie metody wykrywania wirusów oparte o systematycznie aktualizowane bazy sygnatur wrogich programów oraz unikalny zestaw metod zwany zaawansowaną analizą heurystyczną. Dzięki temu połączeniu technologia ThreatSense™ wyjątkowo skutecznie chroni przed wszelkimi typami zagrożeń. Stale aktualizowane bazy sygnatur pozwalają ze 100% precyzją wykrywać i usuwać znane już i sklasyfikowane zagrożenia. Z drugiej strony, zaawansowana analiza heurystyczna jest zdolna do skutecznej walki z zupełnie nowymi, nieznanymi jeszcze wirusami i wrogimi programami gwarantując pełną ochronę typu „day zero protection”. Zaawansowana analiza heurystyczna będąca kluczowym elementem technologii ThreatSense™ wykorzystuje wiele różnych sposobów badania podejrzanych programów (kodów). Wśród nich są takie metody jak pasywna analiza heurystyczna, analiza algorytmiczna, sygnatury generyczne, emulacja oraz metody typu sandbox. Moduł ThreatSense™ doskonale radzi sobie z rzadką grupą wirusów polimorficznych i metamorficznych. Ponadto, wykrywa wirusy w zabezpieczonych hasłem dokumentach MS Office, w plikach skompresowanych tj. ZIP, RAR, ARJ, LZH czy też LHA oraz w chronionych plikach wykonywalnych tj. Pklite, Lzexe, Diet, Exepack, CPAV, UPX oraz AsPack.

### Najszybszy antywirus na rynku

Program NOD32 jest jednym z najszybszych rozwiązań antywirusowych na rynku. Program szybko i skutecznie skanuje pocztę nawet na bardzo obciążonym serwerze, a jego działanie jest dla użytkownika niezauważalne. Wyjątkowa szybkość programu została wielokrotnie potwierdzona w testach. NOD32 skanuje od 2 do 50 razy szybciej niż inne programy antywirusowe. Uzyskanie takiej szybkości skanowania możliwe jest dzięki temu, że moduły kluczowe dla szybkości działania programu zostały napisane i zoptymalizowane w języku niskiego poziomu (assemblerze).

### Sposób działania

NOD32 for MS Exchange skanuje w czasie rzeczywistym całą pocztę przychodzącą i wychodzącą z serwera pocztowego. Skanowane są nie tylko same wiadomości, ale także wszystkie ich załączniki. W przypadku wykrycia wirusa lub innego wrogiego programu w poczcie lub jej załącznikach program podejmuje działanie zgodnie w ustalonymi parametrami i powiadamia o tym fakcie odbiorcę poczty. Możliwe akcje to wyleczenie infekcji, usunięcie zainfekowanego załącznika (Exchange wersja 2000 i 5.5), usunięcie całej wiadomości (Exchange 2003) lub przeniesienie wiadomości i załączników do kwarantanny. Dla zapewnienia właściwego poziomu bezpieczeństwa pliki w katalogu kwarantannie przechowywane są w postaci zaszyfrowanej. Administrator może dodatkowo uruchomić skanowanie zasobów serwera MS Exchange na żądanie. Skanowane są wtedy wszystkie skrzynki pocztowe użytkowników systemu oraz foldery publiczne. NOD32 for MS Exchange chroni nie tylko pocztę i foldery publiczne, ale także w pełni zabezpiecza przed wirusami i wrogimi programami sam serwer. Rezydentny monitor antywirusowy AMON pracujący w tle kontroluje w czasie rzeczywistym wszystkie uruchamiane czy otwierane zbiory. Wszystkie informacje o wykrytych wirusach, wynikach skanowania oraz przeprowadzonych aktualizacjach odnotowywane są w dzienniku zdarzeń.

### ThreatSense.NET

W razie wykrycia przez technologię ThreatSense™ nowego zagrożenia, możliwe jest automatyczne wysłanie podejrzanego pliku do natychmiastowej dalszej analizy w laboratorium ESET-a. W razie potrzeby opracowywane są aktualizacje bazy sygnatur, pozwalające na jednoznaczną identyfikację nowego zagrożenia i jego usunięcie.

### Automatyczna aktualizacja

Aktualizacja bazy sygnatur odbywa się w pełni automatycznie na zasadzie inkrementacji. Niewielkie aktualizacje sygnatur baz wirusów minimalizują obciążenie sieci oraz czas pobierania. Aktualizacje mogą być pobrane przez Internet bezpośrednio z serwera producenta, z wybranego serwera lub stacji roboczej w lokalnej sieci.

### Wymagania systemowe:

MS Exchange Server 5.5 z SP3 lub wyższym  
MS Exchange Server 2000/2003 z SP1 lub wyższym

