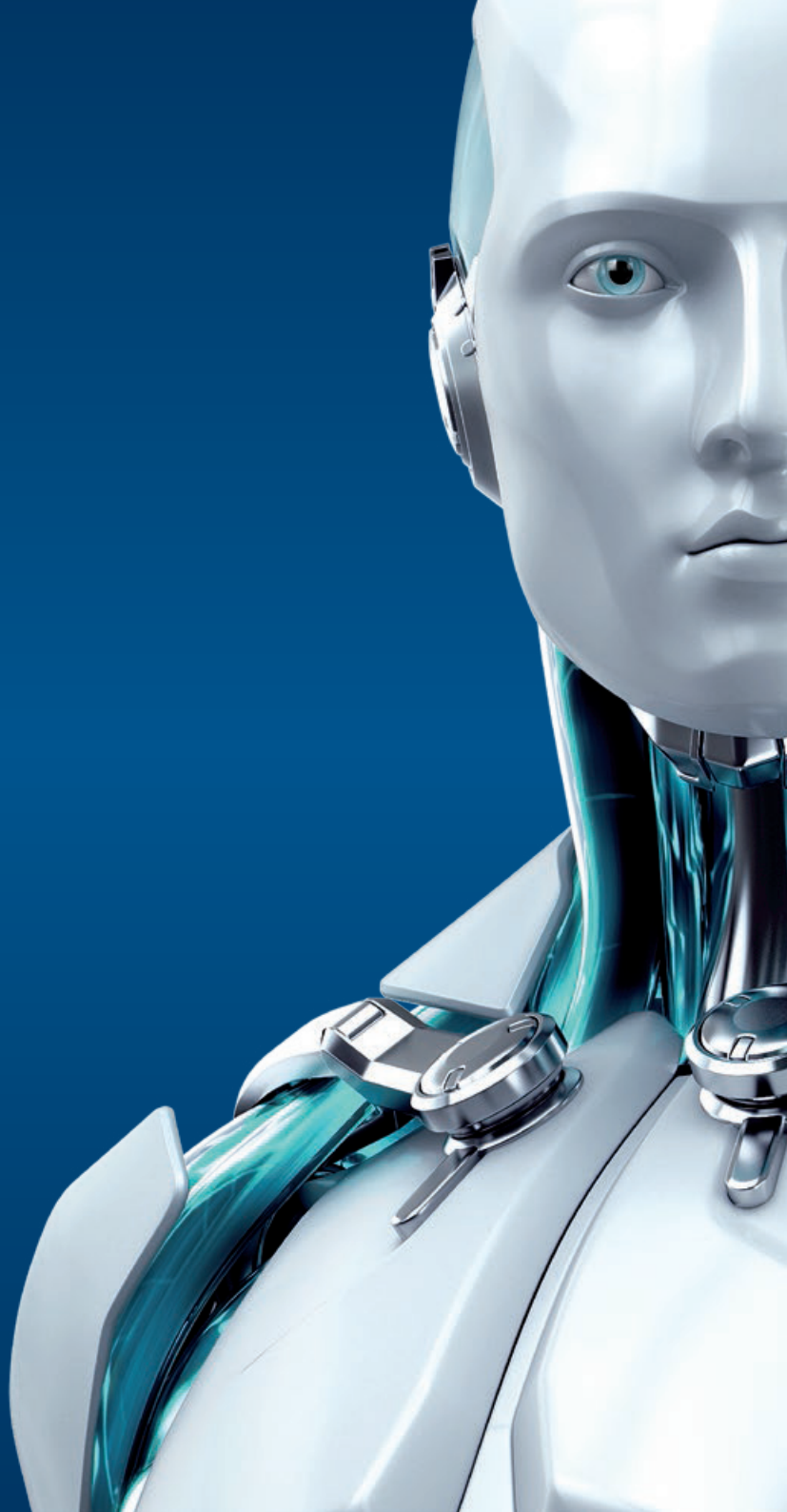
MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

MOŻESZ WIĘCEJ

ENJOY SAFER TECHNOLOGY™



ESET

MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

ESET Mail Security for Microsoft Exchange Server to skuteczne oprogramowanie antywirusowe oraz antyspamowe, które zapewnia ochronę przed szkodliwą zawartością na poziomie serwera pocztowego. Dzięki lekkości rozwiązania serwer pracuje z maksymalną wydajnością. Program wykorzystuje opartą na chmurze technologię ESET Live Grid, dzięki czemu łączy w sobie wysoką prędkość skanowania z najwyższym poziomem bezpieczeństwa.

Rozwiązanie zapewnia kompletną ochronę serwera pocztowego – w tym własnych plików serwera. ESET Mail Security for Microsoft Exchange Server umożliwia zastosowanie polityk bezpieczeństwa na podstawie wykrywania prawdziwych rozszerzeń plików i pozwala na monitorowanie wszystkich ustawień za pomocą webowej konsoli zarządzającej ESET Remote Administrator.

Ochrona przed zagrożeniami i ochrona antyspam

Antywirus i antyspyware	Zabezpieczenie przed wszystkimi rodzajami zagrożeń, m.in. przed wirusami, rootkitami, robakami i oprogramowaniem szpiegującym. Skanowanie w oparciu o chmurę ESET LiveGrid: biała lista bezpiecznych plików bazująca na reputacji obiektów w chmurze dla lepszego i szybszego skanowania. Tylko informacje o plikach wykonywalnych i archiwach wysyłane są do chmury – wysyłane dane są w pełni anonimowe.
Antyspam i Antyphishing	Skutecznie blokuje wiadomości spamowe oraz phishingowe, bez konieczności dodatkowej konfiguracji wyniku spamu SCL (Spam Confidence Level). Bezpośrednio po instalacji produkt gotowy jest do działania bez konieczności dodatkowej konfiguracji.
Lokalne Zarządzanie Kwarantanną	Właściciel każdej skrzynki pocztowej ma możliwość przeglądania zawartości swojej kwarantanny z poziomu przeglądarki internetowej. W zależności od przydzielonych przez administratora uprawnień użytkownik może sortować wiadomości poddane kwarantannie, przeszukiwać jej zawartość lub wykonywać dozwolone akcje. Możliwe do wykonania akcje zależą od powodu, z jakiego dana wiadomość trafiła do kwarantanny. Istnieje możliwość regularnego wysyłania podsumowania kwarantanny do użytkownika, z poziomu którego będzie mógł wykonać odpowiednie akcje.
Skanowanie bazy danych na żądanie	Administrator może wybrać bazy danych, dla których mają być przeskanowane (na żądanie) odpowiednie skrzynki pocztowe. Takie skanowanie może być skonfigurowane w oparciu o czas modyfikacji każdej wiadomości, co pozwala zminimalizować zużycie zasobów serwera.
Zasady przetwarzania wiadomości	Rozwiązanie oferuje szeroki zakres możliwości przetwarzania każdej wiadomości pocztowej. Parametry przetwarzania zawierają standardowe pola takie jak: temat wiadomości, nadawca, tekst, nagłówki wiadomości, ale dodatkowo zawierają możliwość weryfikacji wyników poprzedniego skanowania antyspamowego lub antywirusowego. Wykrywane są również uszkodzone lub zabezpieczone hasłem archiwa oraz pliki z ich oryginalnymi rozszerzeniami. Każda reguła może wykonywać inną czynność.
Blokada programów typu exploit	Blokuje zagrożenia i ataki, które skutecznie unikają wykrycia przez tradycyjne aplikacje antywirusowe. Eliminuje zagrożenia blokujące komputer i wyłudzające okup. Chroni przed atakami, wykorzystującymi luki w przeglądarkach internetowych, czytnikach PDF, komponentach pakietu Office, klientach pocztowych czy oprogramowaniu Java.
Zaawansowany skaner pamięci	Rozbudowuje ochronę antywirusową o skuteczne zabezpieczenie przed skomplikowanymi zagrożeniami, wielokrotnie spakowanymi lub zaszyfrowanymi.
System zapobiegania włamaniom działający na hoście (HIPS)	Oferuje możliwość zdefiniowania odrębnych reguł dla rejestru systemu, procesów, aplikacji i plików.
Kontrola urządzeń	Blokuje nieautoryzowane nośniki. Umożliwia tworzenie reguł w oparciu o grupy użytkowników w celu dopasowania ich do polityki bezpieczeństwa firmy. Program ESET powiadamia użytkownika końcowego o blokadzie urządzenia i umożliwia mu wznowienie dostępu do danych, przy czym informacja o blokadzie zostanie zapisana w dzienniku zdarzeń.

Ochrona rozbudowanych środowisk

Niezależne migawki maszyn wirtualnych	Aktualizacje baz sygnatur wirusów oraz modułów aplikacji ESET mogą być przechowywane poza domyślną lokalizacją. To sprawia, że aktualizacje nie muszą być pobierane ponownie, gdy maszyna jest przywracana do poprzedniego stanu. Mechanizm ten pozwala ograniczyć ilość danych pobieranych z Internetu.
Wsparcie dla klastrowania	Umożliwia skonfigurowanie rozwiązania tak, aby po zainstalowaniu w środowisku klastrowym automatycznie replikowało swoje ustawienia. Intuicyjny kreator pozwala w łatwy sposób przenieść konfigurację pomiędzy wieloma instancjami ESET Mail Security oraz zarządzać nimi jako całością.
Wsparcie dla wirtualizacji	ESET Shared Local Cache przechowuje dane dotyczące skanowanych plików, dzięki czemu nie są one ponownie sprawdzane na innych maszynach wirtualnych. Znacząco zwiększa to wydajność skanowania. Aktualizacje baz sygnatur wirusów i modułów aplikacji ESET przechowywane są poza domyślną lokalizacją, dzięki czemu nie ma konieczności ich ponownego pobierania w przypadku przywrócenia migawki maszyny wirtualnej.
Wsparcie dla Windows Management Instrumentation (WMI)	Zapewnia możliwość monitorowania kluczowych funkcjonalności programu ESET Mail Security za pośrednictwem Windows Management Instrumentation. Pozwala na przesyłanie logów do narzędzi SIEM (wspomagających zarządzanie logami, ich monitoring i raportowanie).

Dostępne pakiety

	OCHRONA KOMPUTERÓW POZIOM ANTIVIRUS	OCHRONA KOMPUTERÓW POZIOM SECURITY	OCHRONA URZĄDZEŃ MOBILNYCH	OCHRONA SERWERÓW PLIKOWYCH	OCHRONA SERWERÓW POCZTOWYCH	OCHRONA BRAMY INTERNETOWEJ
ESET SECURE ENTERPRISE	■	■	■	■	■	■
ESET SECURE ENTERPRISE AV LEVEL	■		■	■	■	■
ESET SECURE BUSINESS	■	■	■	■	■	
ESET SECURE BUSINESS AV LEVEL	■		■	■	■	
ESET ENDPOINT SECURITY SUITE	■	■	■	■		
ESET ENDPOINT ANTIVIRUS SUITE	■		■	■		
ESET ENDPOINT SECURITY	■	■	■			
ESET ENDPOINT ANTIVIRUS	■		■			

BEZPŁATNA POMOC TECHNICZNA

Możesz więcej dzięki pomocy naszych specjalistów. Pomoc techniczna świadczona jest w języku polskim za pośrednictwem telefonu lub poczty mailowej.

Przydatne funkcje

Wykluczenia i wyjątki	Administrator może definiować procesy, które mają być ignorowane przez moduł ochrony w czasie rzeczywistym – wszystkie operacje wykonywane na plikach przez uprzywilejowane procesy będą wtedy uznawane za bezpieczne. Opcja ta jest szczególnie przydatna w przypadku procesów, które szczególnie często nakładają się z ochrona plików w czasie rzeczywistym, np. zadania backupu, migracje maszyn wirtualnych.
Przyrostowe mikroaktualizacje	Regularne aktualizacje pobierane są w postaci małych pakietów inkrementacyjnych. Pozwala to zabezpieczyć zasoby systemowe i pasmo internetowe bez wpływu na wydajność całej infrastruktury sieciowej. Proces aktualizacji nie wpływa na pamięć operacyjną, czy CPU na stacji klienckiej.
Instalacja komponentowa	Oprócz wymaganych komponentów, ESET pozwala wybrać i zainstalować tylko te komponenty, które potrzebujesz: - Ochrona systemu plików w czasie rzeczywistym - Ochrona stron internetowych i poczty e-mail - Kontrola dostępu do urządzeń - ESET Log Collector - i wiele innych
Zdalne zarządzanie	Zdalna instalacja aplikacji, uruchamianie zadań, ustanawianie polityk bezpieczeństwa, zbieranie logów, otrzymywanie powiadomień i przegląd zabezpieczeń sieci - wszystko za pomocą nowej konsoli webowej ESET Remote Administrator.
ESET Log Collector	Gromadzi wszystkie ważne logi w jednym archiwum. Logi mogą być wysyłane na wskazany adres email lub zapisywane na dysku sieciowym.
ESET License Administrator	ESET License Administrator zapewnia jeszcze bardziej przejrzysty widok statusów posiadanych licencji i ich wykorzystania w czasie rzeczywistym. Pozwala administratorowi licencji na połączenie wielu licencji od wielu użytkowników w ramach jednego konta, a także zarządzanie nimi.

Copyright © 1992 – 2015 ESET, spol. s r. o. ESET, ESET logo, postać androida ESET, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo i/lub pozostałe wymienione produkty firmy ESET, spol. s r. o., są zastrzeżonymi znakami towarowymi firmy ESET, spol. s r. o. Windows® jest znakiem towarowym grupy Microsoft. Znaki towarowe DAGMA oraz DAGMA Bezpieczeństwo IT są objęte prawami ochronnymi. Pozostałe wymienione nazwy firmy lub produktów mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli. Wyprodukowano zgodnie ze standardami jakości ISO 9001:2008.

DYSTRYBUCJA W POLSCE:

DAGMA sp. z o.o.
ul. Pszczyńska 15, 40-478 Katowice
tel. 32 259 11 00, faks 32 259 11 90
www.dagma.com.pl

www.eset.pl