

Przedruk

Fragment zredagowany przez G Data

Bezpieczeństwo IT
- produkty dla firm



Przegląd pakietów bezpieczeństwa dla firm, 2009

Język oryginału: angielski

Maj 2009

Data ostatniej wersji dokumentu: 2009-05-27

www.av-comparatives.org

Spis treści



Ryzyko jakie niesie ze sobą złośliwe oprogramowanie 3
Grupa docelowa 4
Testowane produkty 5
Streszczenie 6
Przegląd 8
G Data 9
Podsumowanie 10
Nagroda: „Zatwierdzony produkt dla firm” 12
Zalety i wady 12
Obszary zastosowania 12
Szczegóły testów 13
Lista opcji (fragment) 21
Prawa własności i zastrzeżenia 30

Ryzyko jakie niesie ze sobą złośliwe oprogramowanie



Większość organizacji jest świadoma niebezpieczeństw czyhających na ich środowisko informatyczne. Wirusy, trojany, robaki, exploity i wiele innych zagrożeń stwarza poważne ryzyko dla działu IT. Awaria systemu komputerowego może oznaczać znaczne straty finansowe, a nawet prowadzić do niewypłacalności firmy. Działy IT firm są świadome tego problemu. Jedynym rozwiązaniem jest zaopatrzenie się w najlepszą ochronę przeciwko tym zagrożeniom. Sam program antywirusowy zdecydowanie nie jest wystarczający. Pojawia się zbyt wiele zagrożeń, zaczynając od zainfekowanych wiadomości pocztowych, exploitów itp. Niezbędny jest kompleksowy pakiet ochronny zabezpieczający przed nimi wszystkimi .

Funkcjonalna różnorodność

Z uwagi na ogromną różnorodność funkcjonalną różnych pakietów antywirusowych i produktów dla firm, zdobycie odpowiedniego rozeznania w temacie staje się dla osób odpowiedzialnych za podjęcie decyzji coraz trudniejsze. Który produkt powinien zostać wybrany dla danego obszaru zastosowań?

Naszym głównym kryterium w tych testach nie był jednak stopień wykrywalności zagrożeń, lecz skupiliśmy się na samych produktach, ich obsłudze, przyjazności interfejsu i zakresowi funkcji. W bardzo szczegółowej tabeli przygotowaliśmy zestawienie możliwości oferowanych przez różne produkty.

Aby zobaczyć wskaźniki wykrywalności zagrożeń dla poszczególnych produktów, prosimy odwiedzić naszą stronę internetową:

<http://www.av-comparatives.org> - zakładka „Główne Testy”

Grupa docelowa

Ten raport jest adresowany przede wszystkim do administratorów sieci w różnej wielkości organizacjach. Aby przedstawić pełny przegląd, umieściliśmy tu szczegółową procedurę instalacji. Dzięki temu administratorzy będą mogli dokładnie zrozumieć, jak kolejno postępować. Prezentowany jest jedynie stan na chwilę obecną, gdyż produkty te są ciągle rozwijane i nieustannie aktualizowane.

Sprzęt i oprogramowanie

Rzadko się zdarza by organizacje używały najnowszej wersji sprzętu. Bazując na ankiecie przeprowadzonej przez nas wśród 50 organizacji różnej wielkości, do testów wybraliśmy sprzęt odpowiadający generacji ogólnie wykorzystywanych komputerów. Nasz wybór celowo padł na nieco starsze konfiguracje, aby odzwierciedlić rzeczywisty stan środowiska IT wielu organizacji.

Konfiguracja serwera

CPU:	Dual Xeon
Pamięć RAM:	4 GB RAM
Dysk:	250 GB, S-ATA
System operacyjny:	Windows 2003 Small Business Server zawierający Service Packs i aktualizacje zabezpieczeń aż do 28. lutego 2009 roku
Pełniący rolę serwera:	Kontroler domen z Exchange 2003. DNS łącznie z serwerami przekazującymi

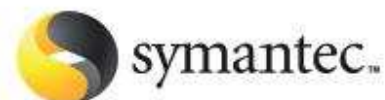
Konfiguracja klienta

CPU:	Intel Pentium IV, 3 GHz
Pamięć RAM:	1 GB RAM
Dysk:	40 GB, S-ATA
System operacyjny:	Windows XP Professional SP3, aktualizacje zabezpieczeń do 28. lutego 2009

Testowane produkty

W przeglądash i testach wzięli udział następujący producenci:

AVIRA	www.avira.com
ESET	www.eset.com
G Data	www.gdata.de
Kaspersky	www.kaspersky.com
Sophos	www.sophos.com
Symantec	www.symantec.com
TrustPort	www.trustport.com



Wszystkie znaki formowe są objęte prawami autorskimi zgłoszonymi przez odpowiadających im producentów.

Streszczenie

Wszyscy, którzy wzięli udział w testach wspaniale wykonali swoje zadanie. Możemy oczekiwać jednego: nasze testy wykazują, że producenci bardzo dobrze odpowiadają na potrzeby pojawiające się wewnątrz organizacji.

Nie ma też żadnych wyjątków. Wszystkie produkty spełniają popularne standardy bezpieczeństwa. Wszelkie decyzje dotyczące zakupu muszą być podjęte w zależności od tego, gdzie produkt ma być później zastosowany. Należy też zwrócić specjalną uwagę na zakres funkcji produktu. Niektóre produkty mogą bardziej odpowiadać przedsiębiorstwom, tj. dużym i bardzo dużym organizacjom, podczas gdy inne mogą być bardziej adekwatne dla przedsięwzięć na małą i średnią skalę, a jeszcze inne doskonale odpowiadać potrzebom indywidualnych użytkowników. Podsumowując, produkty Symantec, Kaspersky oraz G DATA stały się popularnymi produktami uniwersalnymi, podczas gdy AVIRA okazała się dobrym wyborem dla średniej skali przedsiębiorstw. SOPHOS pokazał swoją mocną stronę i doświadczenie jako twórca produktu idealnego dla klientów korporacyjnych, dzięki swojemu wspaniałemu Active Directory. Rozwiązanie przygotowane dla klientów korporacyjnych przez ESET zainteresowało nas przed wszystkim swoim ogromnym potencjałem oferowanym rynkowi przedsiębiorstw. Uważamy też, że Trustport jest idealną propozycją dla małych firm.

Bez wątpienia, SYMANTEC zdobył szerokie doświadczenie w zakresie bezpieczeństwa oprogramowania. Jego pakiet nie pozostawia nic więcej do życzenia. Jedyną uwagą jest dość długi czas instalacji, zwłaszcza tworzenia bazy danych, oraz wymagające poprawienia podstawowe wsparcie dla bazy danych.

Siła G DATA leży w prostocie procedury instalacyjnej. Pakiet ten jest najłatwiejszym do zainstalowania oprogramowaniem. Należy podkreślić także dystrybucję konfiguracji master-slave oraz wzorcowe rozwiązywanie problemu awarii powodującej konieczność przejęcia obowiązków serwera głównego przez serwer rezerwowy. ESET oferuje bezdyskusyjnie największe możliwości konfiguracyjne. Pakiet wspiera też największą liczbę sposobów wdrożenia produktu. Jednakże, w każdym z powyższych przypadków, przed podjęciem decyzji niezbędna jest wcześniejsza dogłębna analiza. Gdy konieczne jest zainstalowanie ponad 50.000 użytkowników, tego pakietu po prostu nie można przeoczyć.

Nawet oprogramowanie dostarczone przez firmę KASPERSKY jest w pełni dopracowanym pakietem, którego główną silną stroną jest obsługa baz danych. Pakiet jest jednym z niewielu produktów obsługujących MySQL. Nawet funkcja logowania, bardzo ważna dla wielu organizacji, została świetnie zaimplementowana.

Konsola zarządzająca firmy ALVIRA, zaprojektowana jako prosta struktura, jest idealną opcją dla małych i średnich przedsiębiorstw. Jest naprawdę prosta i wygodna w obsłudze dla administratora, który musi rozprowadzić oprogramowanie wśród klientów. Konsola administratora prezentuje się przejrzysto dla operacji biznesowych dokonywanych na małą i średnią skalę, jednak w przypadku wykonywania jednakowych operacji w tym samym czasie dla tysięcy klientów staje się nieporęczna i uciążliwa w obsłudze. SOPHOS, z zaimplementowaną obsługą Active Directory, prezentuje się jako firma skoncentrowana na obsłudze organizacji. Posiada niewątpliwie najlepsze wsparcie dla Active Directory. Dzięki temu możliwe jest przenoszenie różnych ról między wieloma osobami w celu administracji systemem

ochrony antywirusowej w środowiskach wymagających wysokiego poziomu bezpieczeństwa, odciążając tym samym administratora.

W przypadku produktu firmy TRUSTPORT, należy zdecydowanie podkreślić hasło „Użyteczność i zarządzanie”. Używanie konsoli jest bardzo łatwe, nawet bez czytania podręcznika użytkownika szybko i sprawnie można odnaleźć wiele potrzebnych funkcji i akcji. Pod tym względem doskonała implementacja i możliwości nawigacji po różnych zarządzających konsolach opracowana przez TRUSTPORT nie pozostawia miejsca dla nawet najmniejszych zastrzeżeń.

Stan

To, co zauważyliśmy przy prawie wszystkich testowanych produktach to bezpretensjonalna implementacja obsługiwanego w czasie rzeczywistym stanu. Dla użytkownika, zwłaszcza w dużych firmach, jest rzeczą niezwykle ważną wiedzieć w każdej chwili, co w danym momencie robi system antywirusowy. Poszukiwanie źródeł problemu staje się znacznie prostsze, jeśli użytkownik jest w stanie w wygodny sposób nadzorować różne moduły i jest na bieżąco informowany o stanie. W testowanych przez

nas produktach najczęściej pomijane jest to, co stało się już standardową opcją dla firewalli.

Ostatecznie, można powiedzieć, że wybierając produkt chroniący przed wirusami, użytkownik nie powinien brać pod uwagę jedynie jego ceny, która, przy podobnych statystykach wykrywalności wirusów, jest porównywalna (co widać w raporcie z testów przeprowadzonych przez nas w lutym, znajdującym się na naszej stronie internetowej). Wręcz przeciwnie, powinien się on skoncentrować na funkcjach, które rzeczywiście są mu niezbędne. Zalicza się do nich prostą obsługę, łatwość instalacji, opcje sortowania ze względu na klientów indywidualnych w dużych firmach, możliwość zdefiniowania nie jednego a wielu serwerów zastępczych na wypadek awarii serwera głównego itd. W załączniku przedstawiliśmy szczegółowy przegląd tych opcji.

Ulepszenia produktów

Producenci dobrze przyjęli wnioski wynikające z naszego przeglądu. Niektóre z ulepszeń zaproponowanych przez nas w tym raporcie zostaną wzięte pod uwagę i zaimplementowane w kolejnych wersjach ich produktów.

Mamy zaszczyt oświadczyć, że wszystkie przedstawione w tym raporcie produkty otrzymały Pieczęć Uznania (Seal of Approval) przyznawaną przez AV-Comparatives. Tak jak można było oczekiwać od produktów antywirusowych przeznaczonych dla odbiorców biznesowych, wszystkie spełniały bardzo dobrze swoje funkcje. Administratorzy IT mogą zauważyć, że niektóre produkty odpowiadają ich potrzebom biznesowym bardziej niż inne, z uwagi na to, że spełniają one specjalne zapotrzebowanie na szukane przez nich grupy opcji.



Przegląd

Staramy się przedstawić przegląd produktów, który może posłużyć w podjęciu decyzji. Jednakże, przed podjęciem decyzji zakupu, bazowanej na tej recenzji, zalecamy wypróbowanie tych produktów na własnym systemie. Wszyscy producenci oferują wersje testowe swoich produktów i posiadają wykwalifikowanych przedstawicieli w większości krajów. Zarówno recenzja jak i poniższa tabela zawierają subiektywne oceny wystawione w czasie testów oraz informacje dostępne powszechnie na stronie producentów.

	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	TrustPort
Instalacja na serwerze	★★★★	★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★
Wdrożenie u klienta	★★★★	★★★★	★★★★	★★★★	★★★★★	★★★★★	★★★
Użyteczność i zarządzanie	★★★	★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★
Osiągi	★★★★★	★★★★★	★★★★★	★★★★★	★★★★	★★★★★	★★★★
Odbiorcy docelowi							
Rynek SOHO	★★★★★	★★	★★★★★	★★★★★	★★★★	★★★★★	★★★★
Małe firmy	★★★★★	★★★★	★★★★★	★★★★★	★★★★	★★★★★	★★★
Średnie firmy	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★
Przedsiębiorstwa	★★★	★★★★★	★★★★	★★★★	★★★★	★★★★★	★★
Podręcznik użytkownika	★★★★	★★★	★★★★	★★★★	★★★★	★★★★	★★★
Obsługa MS AD		★★★★	★★★★	★★★★	★★★★★	★★★★	
Obsługa bazy danych	★★	★★	★★★★	★★★★★	★★★★	★★★★	★
Łatwość instalacji	★★★★★	★★	★★★★★	★★★★	★★★★★	★★★★★	★★★
Logowanie	★★★	★★	★★★	★★★★	★★★★	★★★	★★
Stan w czasie rzeczywistym	★★★★	★★★	★★★	★★★★	★★★★	★★★	★★★★
SPAM	★★★	★★★★★	★★★★★	★★★★	★★★★★	★★★★★	★★★
Wsparcie techniczne	★★★★	★★★★★	★★★★	★★★★★	★★★★★	★★★★★	★★★★
Strona internetowa	★★★★★	★★★★★	★★★★	★★★★★	★★★★	★★★★★	★★★★
Ocena ogólna	★★★★	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★



G Data

Testowane oprogramowanie:

AntiVirusBusiness 10

ClientSecurityBusiness 10

MailSecurity 10



Konsola administratora i ochrona serwera plików

Ochrona klienta

Ochrona serwera pocztowego



Podsumowanie

Strona producenta (www.gdata.de):

Strona jest elegancko zaprojektowana i umożliwia łatwą nawigację. Spełnia też ona popularne standardy internetowe. Menu jest spójne i utrzymane w prostej formie.

Na stronie znajduje się sklep online, który jedynie odsyła do najbliższego przedstawiciela.

System ten posiada własną strefę bezpieczeństwa (wątki), w której można znaleźć przegląd możliwych zagrożeń pochodzących z internetu, wraz ze wskazaniem produktu, który najlepiej przed nimi chroni. Można tam znaleźć szczegółowe informacje dotyczące zagrożeń, natomiast glosariusz ułatwia pracę użytkownikom, którzy jeszcze nie są do końca obeznani ze wszystkimi zagadnieniami.

Przebieg instalacji:

Po pobraniu plików instalacyjnych o niewiarygodnie dużych rozmiarach (2.58 GB) administrator oczekuje eleganckiego kreatora instalacyjnego na wysokim poziomie.

Produktom nadano właściwe, odpowiadające ich przeznaczeniu nazwy – sugerujemy rozpocząć od zapoznania się z nimi.

W pierwszym kroku należy zaktualizować wersję serwera do wersji 3.5 Microsoft .NET.

Aktualizacja ta jest zawarta w programie instalacyjnym pakietu. Niestety, wymagany jest przy tym restart serwera.

Po ponownym uruchomieniu serwera, a przed ustanowieniem połączeń sieciowych rozpoczyna pracę kreator instalacji. Tu kryje się odpowiedź na pytanie, dlaczego pliki instalacyjne dla tego pakietu są takie duże. Kreator instalacji został wspaniale zaprojektowany i nie pozostawia nic do życzenia. System jest w stanie natychmiast wykryć, czy chcesz zainstalować serwer w wersji slave czy w wersji master. Właśnie w tym momencie widać, że pakiet ten jest także odpowiedni dla dużych sieci, posiadających swoje oddziały.

Zapewniona została także dobra obsługa bazy danych. Można wybrać między zintegrowanym mechanizmem bazy danych, nową jednostką serwera SQL czy mechanizmem biurowym MS SQL. Ostatnia propozycja jest również ustawieniem standardowym. Jendakże według nas, wskazówka informująca o tym, że mechanizm biurowy SQL zaleca się w przypadku dużych sieci jest zbędny, zwłaszcza, że dedykowany serwer SQL działa zdecydowanie lepiej, z tym tylko wyjątkiem, że ruch w sieci jest w naturalny sposób zredukowany.

Po zakończeniu instalacji, kreator przeprowadza admina przez proces rejestracji, bez którego niemożliwe jest dokonanie żadnych aktualizacji. Najpierw kreator ustawień wita użytkownika używając powitalnego okienka, które w bardzo elegancki sposób wtapia się w okienko kreatora instalacji.

Nawet tutaj nie znajdujemy żadnych opcji ustawień, których by brakowało. Cały kreator instalacji, od rozpoczęcia aż do zakończenia działania, został zaprojektowany w sposób bardzo zwięzły i prosty w swojej strukturze, sprawiając, że konfiguracja najważniejszych elementów jest kwestią minut.

Według nas, kreator instalacji i kreator pakietu GDATA jest najlepszym dostępnym kreatorem wśród wszystkich testowanych przez nas produktów. Zapewniona jest obsługa Microsoft Active Directory, a standardowe ustawienia zastosowane dla wszystkich modułów praktycznie nie wymagają żadnych modyfikacji.

Konsola administratora:

Konsola jest niesamowicie dobrze zaprojektowana. Bardzo szybko można się w niej odnaleźć, co zawdzięcza podobieństwu do konsoli MMC oraz umieszczonym po prawej stronie zakładkom, które sprawnie doprowadzają użytkownika do interesujących go funkcji.

Konsola została zaprojektowana w sposób niezwykle atrakcyjny i elegancki, co sprawia, że praca z nią jest bardzo przyjemnym doświadczeniem.

Strona pokazująca stan konsoli mogła by być nieco bardziej szczegółowa i zawierać więcej informacji.

Jednakże, tak samo jak w przypadku konsoli stworzonych przez KASPERSKY i SYMANTEC, nie ma powodu do zastrzeżeń odnośnie funkcjonalności i sposobu zorganizowania klientów.

Uważamy, że konsola jest bardzo atrakcyjna i elegancka.

Obszary zastosowania:

Kompletny pakiet G DATA może być wykorzystywany bez żadnych oporów w sieciach o dowolnym rozmiarze. Dzięki konfiguracji master-slave, można też obsługiwać wszystkie oddziały zachowując zasoby sieciowe. Aby dobrze zarządzać dużymi sieciami z pomocą przychodzi baza danych.

Klient AV:

Pojawiające się okienka z wiadomościami nie są nieprzyjemne dla oczu. Po poprawnym zainstalowaniu i uruchomieniu produktu, system wykonuje wszystkie konieczne kroki w sposób automatyczny. Użytkownik posiadający najmniej uprawnień może skonfigurować tylko najważniejsze ustawienia. Również klient został zaprojektowany w sposób atrakcyjny i elegancki. Możliwe jest prawie natychmiastowe rozpoczęcie pracy.

Wnioski:

Produkty G DATA są niezwykle dojrzałe i dobrze zaprojektowane: począwszy od kreatora instalacji, który praktycznie nie stwarza adminowi powodów do wątpliwości, aż do kompleksowych opcji konfiguracji, które biorą pod uwagę wszystkie możliwe potrzeby użytkownika, nawet środowisk bardziej złożonych. Jediną sprawą, co do której można mieć zastrzeżenia to brak funkcji bieżącego zachowywania logów, które pozwoliłyby adminowi zorientować się w bieżącym stanie przebiegu aktualizacji oraz procesu konfigurowania klientów. Dobrze by też było mieć stronę wyświetlającą ogólne informacje, która przedstawiałaby status i poziom zaawansowania konfiguracji klientów.

Jednak pomimo powyższych rozważań, zdecydowanie polecamy pakiet G DATA każdemu administratorowi. Dodatkowo, cena produktu jest bardzo rozsądna.

Nagroda: „Produkt zatwierdzony dla firm”



Zalety i wady

- + Bardzo dobry kreator, który w doskonały sposób prowadzi użytkownika przez proces instalacji
- + Obsługa MS Active Directory
- + Szybka instalacja klienta
- + Konsola administratora zaprojektowana w sposób przejrzysty i spójny
- + Bardzo prosta zdalna instalacja
- + Instrukcja obsługi nie jest konieczna
- + Użyteczny także przy znacznym rozszerzaniu rynku
- + Porządne wsparcie ze strony bazy danych
- + Dobra jakościowo strona internetowa producenta
- Brak strony podsumowania w MMC
- Brak odpowiedniej opcji logowania w czasie rzeczywistym

Obszary zastosowania

Małe sieci (0-50 użytkowników)	Średnie sieci (50-500 użytkowników)	
★★★★★	★★★★★	★★★★

Kreator instalacji	★★★★★
Prowadzenie użytkownika	★★★★
	★★★★★
	★★★
	★★★★
	★★★★
	★★★★
	★★★★
	★★★★
	★★★★

Szczegóły testów

Przebieg instalacji:

Pobieranie produktów:

Menu dostarczone przez producenta zaprojektowane jest w sposób spójny i utrzymane w prostej formie. Nie ma problemu ze znalezieniem konkretnego produktu. Możliwe jest też pobranie każdego z produktów w pełnej wersji funkcjonalnej.

Po poprawnej rejestracji, za pośrednictwem internetu można otrzymywać aktualizacje.

Wykorzystując połączenie o prędkości 1.29 MB/sekundę, pobieranie trwa jak przedstawiono poniżej:

AntiVirus Business 10 (1.06 GB)

⇒ 19:20 min

ClientSecurity Business 10 (1.24 GB)

⇒ 20:20 min

MailSecurity 10 (250 MB)

⇒ 03:12 min

Instalacja produktów:

Jak to sugerują znaczne rozmiary plików, wszystkie produkty przeznaczone dla serwera powinny być zainstalowane z wykorzystaniem kreatora instalacji.



Przedstawione tu menu jest przykładowe, a indywidualne moduły zostały wyposażone w szczegółowe i pełne wyjaśnienia. Dzięki kompozycji modułów i dostępnym dla nich objaśnieniom, kolejne kroki, które należy wykonać, aby przeprowadzić instalację stają się oczywiste.

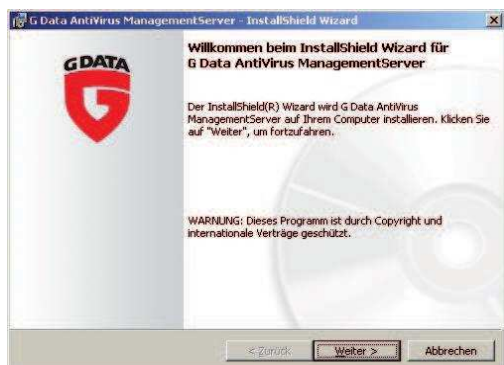
Rozpoczynamy od instalacji serwera zarządzającego (Management Server).



Wymaga on najnowszej wersji Microsoft .NET. Aktualizacja ta jest zawarta w pakiecie instalacyjnym, nie jest więc konieczne pobieranie go.



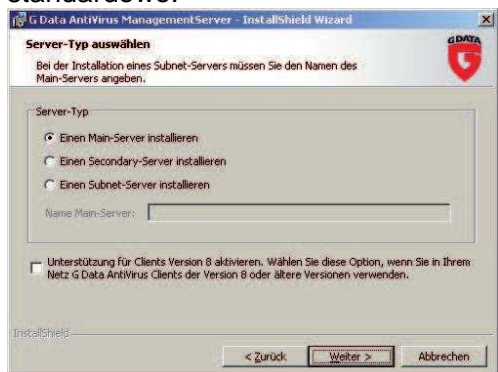
Administratorzy nie lubią, gdy pojawiają się takie wiadomości, ponieważ w tym momencie sieć jest w stanie normalnej pracy. Jednakże ponowne uruchomienie jest konieczny tylko wtedy, gdy .net Framework nie był wcześniej zainstalowany.



Kreator instalacji powraca zaraz po tym, jak zainstalowany zostanie poprawnie MS .net 3.5 i serwer zostanie ponownie uruchomiony.



W zapytaniu o umowę licencyjną i katalog instalacyjny wykorzystujemy wartości standardowe.



W następnym kroku należy wybrać typ serwera. Można natychmiast zauważyć, że nie ma żadnego problemu z wdrożeniem pakietu G DATA w przypadku dużych sieci, posiadających oddziały i zdecentralizowane serwery. Ponieważ jest to pierwsza instalacja w naszej sieci, wybieramy „Serwer główny”.

W następnym kroku wybieramy serwer dla bazy danych pakietu. Wiadomość o tym, że SQL Express jest zalecana w przypadku dużych sieci jest w pewnym sensie myląca. Ma ona zastosowanie jedynie w przypadku, gdy w istniejącej sieci nie występuje żadna instancja serwera SQL lub też istniejący serwer SQL ma wystarczająco dużo pracy z istniejącymi bazami danych. Trzeba tu jednakże nadmienić, że jeśli chodzi o osiągi, wariant Express serwera MS SQL w przypadku dużych sieci jest oczywiście bezkonkurencyjny.

System ten nie zapewnia obsługi baz danych należących do otwartego oprogramowania, takich jak MySQL.



Właśnie dlatego potężny kreator instalacyjny pakietu G DATA zawiera zestawy instalacyjne MS SQL Server Express.



W następnym kroku należy podać nazwę, pod którą serwer zarządzający będzie dostępny w sieci.

Instalację można rozpocząć, gdy wszystkie informacje zostaną zebrane.



Po poprawnym zakończeniu instalacji po raz kolejny pojawia się wiadomość o rejestracji, która umożliwi systemowi akceptować aktualizacje.



Zaraz po zakończeniu instalacji, pojawia się „Kreator ustawień”:

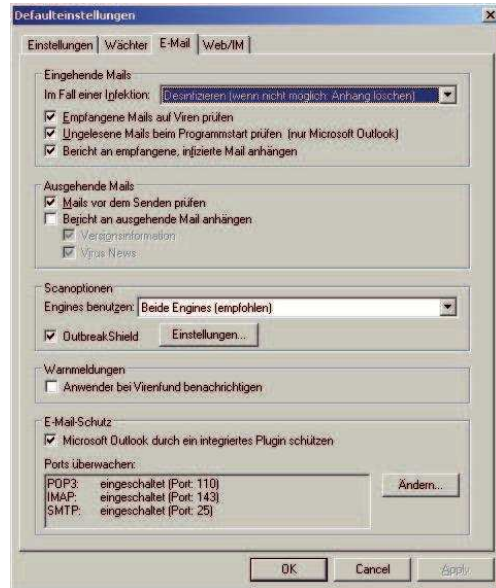
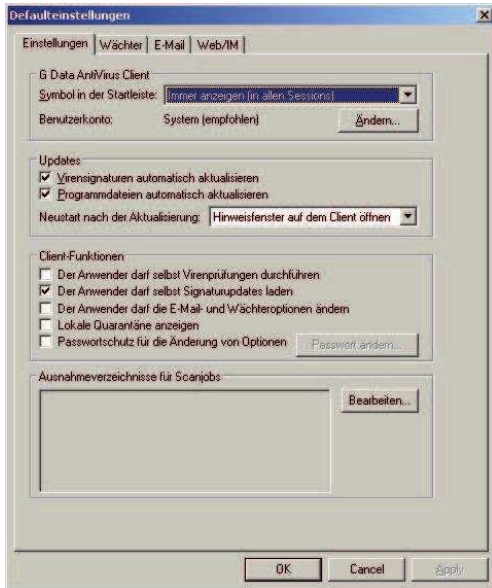


zapomnieć o instrukcji użytkownika jako pomocy przy instalacji.



Bazując na otoczeniu sieciowym i AD, kreator wyświetla te komputery, które nie mają jeszcze zainstalowanych produktów GDATA, jednakże bez konieczności wykonywania jakiegokolwiek specjalnej akcji przy konfiguracji. Opis różnych menu jest wzorowy i właściwie można zupełnie

Z pomocą kreatora można z powodzeniem skonfigurować standardowe ustawienia.

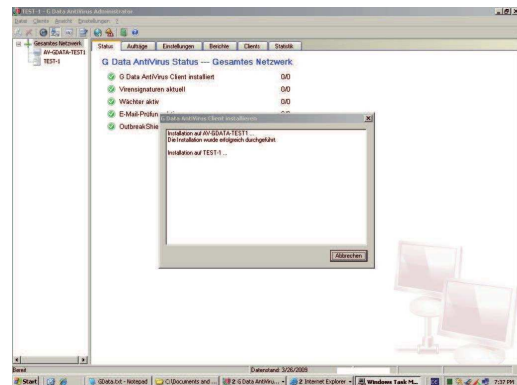


Kreator nie budzi żadnych zastrzeżeń – jest skonstruowany w prosty sposób, zawierając jednocześnie wszystkie niezbędne elementy.



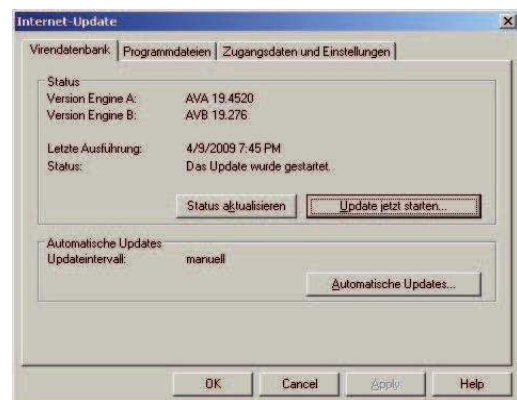
Tutaj konieczne jest zdefiniowanie konta, z wykorzystaniem którego zostaną zainstalowani i skonfigurowani klienci. System zapewnia obsługę MS AD.

W następnym kroku można określić adres poczty elektronicznej, na który powinny być wysyłane wiadomości. Adres ten jest użyty dla porównania z G DATA Internet Ambulance.



Po zakończeniu pracy przez kreator ustawień, można rozpocząć instalację oprogramowania dla wybranych wcześniej klientów i serwerów.

Możliwe jest też określenie osobnego adresu dla wiadomości alarmowych. Jak widać, pakiet G DATA czuje się bardzo swobodnie nawet w środowiskach o skomplikowanych zabezpieczeniach i daje administratorowi możliwość optymalnego skonfigurowania własnego działu biorąc pod uwagę zagadnienia i problemy bezpieczeństwa.



Ustawienia dla metody aktualizacji zostały zaprojektowane jako spójne i utrzymane w prostej formie.

Nawigacja w obrębie konsoli zarządzającej nie pozostawia nic do życzenia, dodatkowo posiada także własny opis. Została utrzymana w skromnej i prostej konwencji, a jednak zawiera wszystkie niezbędne elementy.

W następnym kroku instalowana jest ochrona dla serwera pocztowego.



Po zakończeniu standardowej instalacji, zawierającej typowe zapytania o umowę licencyjną i katalog docelowy, pojawia się okno logowania w konsoli administratora poczty.



Aby móc statystycznie oszacować ruch poczty elektronicznej, konieczne jest umieszczenie tu jednostki SQL-owej.

Można oczywiście wykorzystać zainstalowany już wcześniej serwer SQL Express.

Także Gmail od razu wykrywa, że antywirusowy klient GDATA został już zainstalowany na serwerze i potem wykorzystuje jego sygnatury.

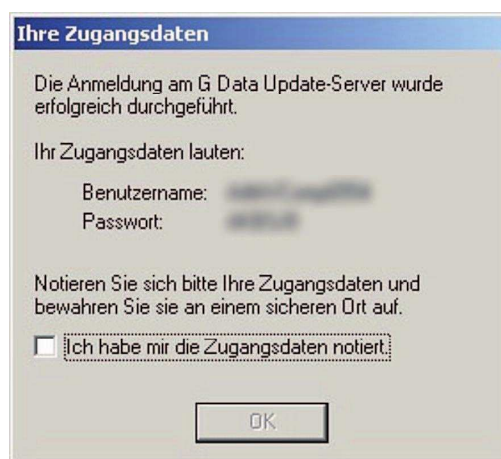


Bezpośrednio po zalogowaniu się do konsoli administratora dla Gmail Security Scanner, prezentowany przegląd aktualnie wykonywanych procesów i inne informacje systemowe:



Także i tutaj interfejs użytkownika nie budzi żadnych zastrzeżeń jeśli chodzi o wygląd przyjazny dla użytkownika przy jednoczesnym zachowaniu możliwości skonfigurowania wszystkich niezbędnych ustawień.

Na koniec wyświetlona zostanie wiadomość o poprawnej rejestracji serwera aktualizacji GDATA:



Lista opcji (fragment)

Lista opcji (fragment)	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Produkt polecany dla sieci:							
do 5 klientów, serwer	Avira AntiVir Professional	ESET Smart Security	G Data Antivirus Business	Kaspersky Small Office Security	Sophos Computer Security (Small Business Edition)	Norton Internet Security	TrustPort PC Security
do 25 klientów i 1 serwer plików	Avira NetWork Bundle	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Business Space Security	Sophos Computer Security (Small Business Edition)	Symantec Endpoint Protection Small Business Edition	TrustPort PC Security z TrustPort Net Gateway
do 25 klientów, serwer plików i serwer komunikacyjny	Avira NetWork Bundle	ESET Smart Security Business Edition and Messaging Bundle	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	Sophos Computer Security (Small Business Edition)	Symantec Protection Suite Small Business Edition	TrustPort PC Security z TrustPort Net Gateway
ponad 25 klientów, więcej niż 1 serwer plików, więcej niż 1 serwer komunikacyjny	Avira AntiVir Business Bundle	ESET Smart Security Business Edition i ESET Mail Security (lub ESET NOD32 Antivirus dla MS Exchange)	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	Sophos Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security z TrustPort Net Gateway
Features Management Server							
Jaka jest całkowita maksymalna liczba klientów?	20,000	bez ograniczeń	50,000	bez ograniczeń	bez ograniczeń	bez ograniczeń	20,000
Jaka jest maksymalna liczba klientów, którzy mogą być obsługiwani pojedynczym serwerem zarządzającym?	20,000	10,000	1,000	20,000	25,000	50,000	2,000
Minimalne wymagania sprzętowe (CPU/pamięć/dysk)		Wystarczający dla systemu operacyjnego i, opcjonalnie, dla bazy danych	Core 2 Duo 2 GB RAM 1,5 GB	Intel Core 2 Duo E8400, 3,00 GHz, 4 GB RAM, HDD SATA 300 GB	Dual/4GB/Raid 0+1	2 GB, pojedynczy procesor (< 10.000 klientów) i 4 GB, dual procesor (> 10.000 użytkowników)	P4/1GB/0.5-3.0 GB
Czy produkt posiada mechanizm zabezpieczający przed aktualizacjami wykorzystującymi drogę połączenia, jak np.UMTS?		konfigurowalne	konfigurowalne			•	
Czy produkt posiada mechanizm aktualizacji delta?	•	•	•	•	•	•	•
Jakie zabezpieczenia posiada produkt, dla zapewnienia, że tylko uprawnione osoby mogą administrować produktem?	Identyfikacja za pomocą nazwy użytkownika i hasła	Zabezpieczenie hasłem, szyfrowane przesyłanie danych	Hasło administratora	Identyfikacja za pomocą nazwy użytkownika i hasła	Zabezpieczenie hasłem, szyfrowane przesyłanie danych, osobna funkcja administratora	Identyfikacja / szyfrowanie	Nazwa użytkownika/ hasło na stronach szyfrowanych SSL
Komunikacja klient/serwer							
Czy klient przeprowadza identyfikację serwera?	•	•	•	•	•	•	
Czy serwer przeprowadza identyfikację klienta?	•	•	•	•	•	•	
Czy dane przesyłane między klientem i serwerem są szyfrowane?	•	•	•	•	•	•	
Czy produkt obsługuje tryb komunikacji wymagającej aktywności klienta ('pull')?	•	•	•	•	•	•	•
Jaki jest zalecany interwał czasowy między komunikatami?	60 minut	5 minut	5 minut	15 minut	w czasie rzeczywistym	5 minut	60 minut
Czy produkt obsługuje tryb komunikacji 'push'?	•	•	•	•	•	•	•
Czy produkt chroni sam siebie przed manipulacjami ze strony użytkownika końcowego lub niebezpiecznego oprogramowania?	•	•	•	•	•	•	
Zapobiega przed zatrzymaniem procesów	•	•	•	•	•	•	
Zapobiega przed modyfikacją lub usuwaniem plików	•	•	•	•	•	•	

Test dla firm 2009 – maj 2009

Serwer proxy							
Dla HTTP	•	•	•	•	•	•	•
Czy produkt obsługuje uwierzytelnianie serwera proxy?	•	•	•	•	•	•	•
Serwer typu master-slave							
Wiele serwerów AV		•	•	•	•	•	•
Serwer typu master kontroluje serwery typu slave znajdujące się w innych biurach		•	•	•	•	•	•
Serwer typu slave do dystrybucji aktualizacji		•	•	•	•	•	•
Instalacja klienta							
Jakie metody wdrażania klienta są obsługiwane przez product?							
Czy produkt zawiera mechanizm wysyłania oprogramowania do klientów?	•	•	•		•	•	•
Czy produkt obsługuje tworzenie pojedynczego wykonywalnego pliku instalacyjnego (.exe)?	•	•	•	•	•	•	•
Które opcje mogą zostać ustawione za pomocą interfejsu użytkownika dla instalacji klienta?							
Czy produkt pozwala administratorowi zdefiniować w interfejsie użytkownika opcje instalacyjne?	•	•	•		•	•	•
Ogólne możliwości							
Czy system ma możliwość obsługi wielu najemców (multi-tenancy)?			•	•	•	•	•
Czy produkt pozwala administratorom określać różne strategie działania dla różnych grup komputerów?	•	•	•	•	•	•	•
Rozpoznawanie lokalizacji							
Czy produkt ma możliwość używania różnych strategii działania, ustawień i zasad w zależności od lokalizacji komputera?	•		•	•	•	•	
Jakie ustawienia/strategie działania mogą zostać zmienione w zależności od lokalizacji?							
Strategie ochrony technologii							
Strategie ochrony antywirusowej	•		•	•		•	•
Strategie zapory sieciowej			•	•	•	•	•
Inne strategie ochrony technologii	Aktualizacje		Antyspam	Antyspam; aktualizacje	Aktualizacje		Niszczarka danych
Konfiguracja interfejsu użytkownika	•		•	•		•	•
Ustawienia wymiany danych			•	•		•	•
Ustawienia aktualizacji zawartości	•		•	•	•	•	•
Klient ma możliwość zdefiniować 'nieograniczoną' liczbę lokalizacji?			•	•		•	
Microsoft Exchange							
Zasoby sieciowe	•	•	•	•	•	•	•
Pamięć systemu / procesy	•		•	•	•	•	•
Sektory ładujące	•	•	•	•	•	•	•
Poczta elektroniczna							
Czy produkt skanuje istniejące wiadomości poczty elektronicznej przechowywane w następujących aplikacjach?							
Microsoft Outlook	•	•	•	•	•	•	
Microsoft Outlook Express	•	•	•	•	•		
Lotus Notes			•			•	
Thunderbird		•	•		•		
The Bat!			•	•			
Czy produkt sprawdza przychodzące i wychodzące wiadomości poczty elektronicznej i załączniki dla następujących protokołów?							
SMTP / POP3	•	•	•	•	•	•	•

IMAP	•	•	•	•	•	•	•
Pliki zarchiwizowane							
ZIP/RAR/ARJ i zarchiwizowane pliki instalacyjne	•	•	•	•	•	•	•
Jak głęboko w strukturę katalogów	20	10	100	bez ograniczeń	5	10	10
Skanowanie na żądanie							
Czy administrator może zdefiniować czas rozpoczęcia skanowania?	•	•	•	•	•	•	•
Czy można zdefiniować wpływ na system ze względu na szybkość skanowania?	•	•	•	•	•	•	•
Skanowanie ze względu na dostęp							
Czy administrator może wyszczególnić, które skanowane lokalizacje powinny zostać dołączone / wykluczone?		•	•	•	•	•	tylko wykluczanie
Pliki / katalogi		•	•	•	•	•	•
Logowanie							
Jakie informacje są zachowywane?							
Data i godzina wykrycia infekcji	•	•	•	•	•	•	•
Nazwa infekcji oraz pierwsza lokalizacja, w której infekcja została wykryta	•	•	•	•	•	•	•
Komputer, który został zainfekowany	•	•	•	•	•	•	•
Podjęta akcja i aktualny stan infekcji	•	•	•	•	•	•	•
Obecna lokalizacja zainfekowanego pliku	•	•	•	•	•	•	•
Skanowanie, które wykryło infekcję	•	•	•	•	•	•	•
Powiadomianie użytkownika końcowego							
Przez wyświetlenie wyskakującego okienka lub balonika	•	•	•	•	•	•	•
Przez dodanie ostrzeżenia w tekście lub temacie zainfekowanej wiadomości pocztowej	•	•	•	•	•	•	•
Przez zastąpienie zainfekowanego załącznika			•	•		•	•
Jakie specjalne akcje może wykonywać produkt?							
Wprowadzenie kwarantanny lokalnego systemu	•	•	•	•	•	•	•
Wprowadzenie kwarantanny centralnej lokalizacji		•	•	•	•	•	
Możliwości ogólne							
Czy zapora sieciowa monitoruje połączenia TCP i UDP (funkcja stateful firewall)?		•	•	•	•	•	•
Reguły zapory sieciowej							
Typ adaptera sieciowego							
Ethernet / Bezprzewodowy			•	•		•	•
VPN			•	•		•	
Modem			•	•		•	•
Protokół							
TCP/UDP/ICMP		•	•	•	•	•	•
Inny			IGMP, GGP, GUP; IDP, GRE		PPTP	Dowolny protokół	
Jakie akcje mogą zostać podjęte w przypadku wywołania reguły zapory sieciowej?							
Zezwolenie / zablokowanie ruchu		•	•	•	•	•	•
Zapytanie użytkownika końcowego		•	•	•	•	•	•

Zarządzanie klientami							
Interfejs klienta-użytkownika							
Czy administrator może kontrolować zmiany w konfiguracji?	•	•	•	•	•	•	•
Czy dla różnych komputerów można zastosować różne strategie działania?	•	•	•	•	•	•	•
W zależności od przynależności do grupy danego komputera	•	•	•	•	•	•	•
Akcje							
Jakie akcje można zainicjować korzystając z konsoli administratora?							
Aktualizacja sygnatur	•	•	•	•	•	•	•
Skanowanie komputera	•	•	•	•	•	•	•
Włączenie skanowania ze względu na dostęp (OnAccess)	•	•	•	•	•	•	•
Aktywacja/dezaktywacja zapory sieciowej	•	•	•	•	•	•	•
Na jakich systemach można zainicjować akcje?							
Pojedynczy komputer	•	•	•	•	•	•	•
Grupa komputerów	•	•	•	•	•	•	•
Czy istnieje konsola dostępna przez internet?	•	•	•	•	•	•	•
Zarządzanie administratorami							
Prawa							
Czy produkt zezwala na wielu administratorów?	•	Jeden na serwer	•	•	•	•	Wielu audytorów, jeden administrator
Kwarantanna							
Katalog kwarantanny							
Czy istnieje scentralizowany katalog kwarantanny?	•	•	•	•	•	•	•
Czy klient posiada swój katalog kwarantanny?	•	•	•	•	•	•	•
Wiadomości							
Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange
Wykrywanie złośliwego oprogramowania							
Skanowanie rekurencyjne w czasie rzeczywistym wszystkich wiadomości i załączników sterowane czasowo i zdarzeniowo	•	•	•	•	•	•	•
Obsługa automatycznych aktualizacji wzorców wirusów	•	•	•	•	•	•	•
Skanowanie tekstu wiadomości i jej załączników	•	•	•	•	•	•	•
Wykrywanie załączników za pomocą wzorca plików, typu plików lub nawet plików modyfikowanych	•	•	•	•	•	•	•
Stosowanie restrykcji dla archiwów takich jak zip, rar	•	•	•	•	•	•	•
Automatyczne wykrywanie nowych skrzynek pocztowych	•	•	•	•	•	•	•
Sprawdzanie pod kątem wirusów zaszyfrowanych wiadomości z wykorzystaniem Crypt	•	•	•	•	Opcjonalne	•	•
Antyspam							
Blokowanie niepożądanych nadawców wiadomości/niepożądanych odbiorców	•	•	•	•	•	•	•
Wykorzystanie aktualnego wzorca spamu do szybkiego rozpoznania nowych spammerskich sztuczek	•	•	•	•	•	•	•
Indywidualne dla każdego użytkownika zarządzanie białymi i czarnymi listami	•	•	•	•	•	•	•

służącymi do blokowania niechcianej korespondencji							
Elastyczne powiadamianie o zablokowanych wiadomościach przekazywane do administratora lub nadawcy/odbiorcy	•		•		•	•	
Wiadomości – przegląd opcji	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows
Wykrywanie złośliwego oprogramowania							
Skanowanie rekurencyjne w czasie rzeczywistym wszystkich wiadomości i załączników sterowane czasowo i zdarzeniowo		•	•	•	•		•
Skanowanie magazynu informacji na każdym serwerze				•	•		
Obsługa automatycznych aktualizacji wzorców wirusów	•	•	•	•	•		•
Skanowanie tekstu wiadomości i załączników	•	•	•	•	•		•
Wykrywanie załączników za pomocą wzorca plików, typu plików lub nawet plików modyfikowanych			•	•	•		
Stosowanie restrykcji dla archiwów takich jak zip, rar			•	•	•		•
Automatyczne wykrywanie nowych skrzynek pocztowych			•		•		
Sprawdzanie pod kątem wirusów zaszyfrowanych wiadomości z wykorzystaniem Crypt			•	•			
Antyspam							
Blokowanie niepożądanych nadawców wiadomości/niepożądanych odbiorców			•		•		•
Wykorzystanie aktualnego wzorca spamu do szybkiego rozpoznania nowych spawerskich sztuczek			•		•		•
Indywidualne dla każdego użytkownika zarządzanie białymi i czarnymi listami służącymi do blokowania niechcianej korespondencji			•				•
Elastyczne powiadamianie o zablokowanych wiadomościach przekazywane do administratora lub nadawcy/odbiorcy			•		•		•
Wiadomości – przegląd opcji	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux
Wykrywanie złośliwego oprogramowania							
Skanowanie rekurencyjne w czasie rzeczywistym wszystkich wiadomości i załączników sterowane czasowo i zdarzeniowo		•	•	•	•		
Obsługa automatycznych aktualizacji wzorców wirusów		•	•	•	•		
Skanowanie tekstu wiadomości i załączników		•	•	•	•		
Wykrywanie załączników za pomocą wzorca plików, typu plików lub nawet plików modyfikowanych		•	•		•		
Stosowanie restrykcji dla archiwów takich jak zip, rar		•	•	•	•		
Automatyczne wykrywanie nowych skrzynek pocztowych		•	•		•		

Test dla firm 2009 – maj 2009

Sprawdzanie pod kątem wirusów zaszyfrowanych wiadomości z wykorzystaniem Crypt			•		Opcjonalnie		
Antyspam							
Blokowanie niepożądanych nadawców wiadomości/niepożądanych odbiorców		TAK (nadawcy), NIE (odbiorcy)	•	•	•		
Wykorzystanie aktualnego wzorca spamu do szybkiego rozpoznania nowych spammerskich sztuczek		•	•	•	•		
Indywidualne dla każdego użytkownika zarządzanie białymi i czarnymi listami służącymi do blokowania niechcianej korespondencji		•	•	•	•		
Elastyczne powiadomianie o zablokowanych wiadomościach przekazywane do administratora lub nadawcy/odbiorcy			•	•	•		
Wsparcie techniczne							
Zdalna kontrola pulpitu	•	•	•	•	•	•	•
Wsparcie za pomocą poczty elektronicznej	•	•	•	•	•	•	•
Serwis u klienta?	•	•	•	•	•	•	Dostępny tylko w Czechach
Obsługa							
Usługi zarządzania, u Producenta		Możliwe u przedstawiciela	Możliwe u przedstawiciela	•		•	
Ceny							
Scenariusz A: 5 klientów, serwer, outlook obsługujący pocztę elektroniczną							
Zalecany produkt	Avira AntiVir Professional	ESET Smart Security	G Data AntiVirus MultiUser	Kaspersky Small Office Security	Sophos Computer Security (Small Business Edition)	Norton Internet Security pakiet dla 5 użytkowników	TrustPort PC Security
1 rok (cena w Euro)	175	119	74	167	243	80	95
3 lata (cena w Euro)	350	235	195	350	485	niedostępne	199
Scenariusz B (małe i średnie firmy): 1 serwer SBS 2003, 25 klientów							
Zalecany produkt	Avira NetWork Bundle	ESET Smart Security Client/ Server/Messaging Bundle	G Data AntiVirus Enterprise	Kaspersky Business Space Security	Sophos Security Suite (Small Business Edition)	Symantec Protection Suite Small Business Edition	TrustPort PC Security with TrustPort Net Gateway
Plan na 1 rok (cena w Euro)	1,015	735	1,342	715	1,381	2,109	1,030
Plan na 3 lata (cena w Euro)	2,030	1,544	2,309	1,609	2,762	niedostępne	2,162
Scenariusz C: 1 serwer plików, 1 serwer Exchange, 200 klientów							
Zalecany produkt	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus dla Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
Plan na 1 rok (cena w Euro)	8,600	5,236	8,060	5,165	7,550	14,421	5,408
Plan na 3 lata (cena w Euro)	17,200	11,000	13,744	11,621	15,100	niedostępne	11,367
Scenariusz D: 2 serwery plików, 1 serwer Exchange, 1000 klientów							
Zalecany produkt	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus dla Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
Plan na 1 rok (cena w Euro)	27,090	17,060	23,951	18,642	25,250	56,770	16,800
Plan na 3 lata (cena w Euro)	54,180	35,820	39,839	41,953	50,500	niedostępne	35,280
Scenariusz E: 10 serwerów plików, 10 serwerów Exchange, 10000 klientów							
Zalecany produkt	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus dla Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
Plan na 1 rok (cena w Euro)	163,400	131,600	190,380	135,069	Odmówiono podania ceny	334,234	102,400
Plan na 3 lata (cena w Euro)	326,800	274,600	316,030	303,806	Odmówiono podania ceny	niedostępne	209,040

	AVIRA			ESET			G Data			Kaspersky			Sophos			Symantec			TrustPort		
Obsługiwany system operacyjny	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony	Serwer zarządzający	Konsola zarządzająca	Klient ochrony
Windows XP																					
Home		•	•	•	•	•	•	•	•		•	•	•	•	•		•	•	•	•	•
Professional		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Professional 64 Bit Intel		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Media Center				•	•	•	•	•	•				•	•	•			•	•	•	•
Media Center 2004				•	•	•	•	•	•				•	•	•			•	•	•	•
Media Center 2005				•	•	•	•	•	•				•	•	•			•	•	•	•
Tablet PC Edition				•	•	•	•	•	•				•	•	•			•	•	•	•
Embedded				•	•	•	•	•	•				•	•	•			Nie wszystkie opcje			
Windows Server 2003																					
Standard	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Enterprise 32/64 Bit	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Data Center 32/64 Bit	•			nietestowane	nietestowane	nietestowane	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Small Business Server	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Cluster Server				nietestowane	nietestowane	nietestowane	•	•	•				•	•	•	•	•	•			
Storage Server				•	•	•	•	•	•				•	•	•	•	•	•			
Web Edition				•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Windows Vista																					
Home Basic 32/64 Bit		•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
HomePremium 32/64 Bit		•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Business 32/64 Bit		•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Ultimate 32/64 Bit		•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Windows Server 2008																					
Standard 32/64 Bit	•			•	•	•	•	•	•	•	•	Tylko KAV dla WSEE	•	•	•	•	•	•	•	•	•

	AVIRA			ESET			G Data			Kaspersky			Sophos			Symantec			TrustPort		
Standard 32 Bit - Core Installation	●			Tylko linia komend	Tylko linia komend	Tylko linia komend	●	●	●			Tylko KAV dla WSEE	●	●	●			●	●	●	●
Standard 64 Bit - Core Installation	●			Tylko linia komend	Tylko linia komend	Tylko linia komend	●	●	●			Tylko KAV dla WSEE	●	●	●	●	●	●	●	●	●
Enterprise 32/64 Bit	●			●	●	●	●	●	●	●	●	Tylko KAV dla WSEE	●	●	●	●	●	●	●	●	●
Data Center 32/64 Bit	●			nietestowane	nietestowane	nietestowane	●	●	●	nietestowane	nietestowane	Tylko KAV dla WSEE	●	●	●	●	●	●	●	●	●
Web Edition 32/64 Bit	●			●	●	●	●	●	●	nietestowane	nietestowane	Tylko KAV dla WSEE	●	●	●	●	●	●		●	
Foundation 32/64 Bit				●	●	●	●	●	●				●	●	●			●		●	
HPC 32/64 Bit				nietestowane	nietestowane	nietestowane	●	●	●				●	●	●					●	
Linux																					
Redhat																					
Redhat Enterprise Linux 5.x 32/64 Bit						●			●		●	●			●			●			
SUSE																					
SUSE Linux Enterprise Desktop 10.x 32/64 Bit						●			●		●	●			●			●			
SUSE Linux Enterprise Server 10.x 32/64 Bit						●			●		●	●			●			●			
Baza danych																					
Czy produkt wymaga bazy danych?	●			TAK, wbudowana i obsługuje kilka innych			●	●		●			●			●			TAK, wbudowana (wykorzystuje własne rozwiązanie)		
Dla ilu użytkowników/klientów zalecana jest darmowa baza danych?							Nieograniczony	Nieograniczony		5000						5000			2000		

	AVIRA			ESET			G Data			Kaspersky			Sophos			Symantec			TrustPort		
Jaka baza danych jest dołączona do pakietu (np. Microsoft SQL, Sybase, MySQL itd.) ?				Microsoft Access (jet)			SQL Express	SQL Express		Microsoft SQL			MSDE SQL			Sybase					
Jakie dodatkowe bazy danych są obsługiwane?																					
Microsoft SQL Server																					
Microsoft SQL Server 2000							•	•		•						•	•				
Microsoft SQL Server 2005				•			•	•		•						•	•				
Microsoft SQL Server 2008										•						•					
Serwer poczty elektronicznej																					
Microsoft Exchange	•					•	•	•			•	•	•			•					
Domino						•	•	•			•	•	•			•					
Tobit						nietestowane	•	•													
Linux						•	•	•			•	•	•								
Mac							•	•			•	•									

Prawa własności i zastrzeżenia



Ta publikacja jest objęta prawem autorskim © 2009 przez AV-Comparatives e.V. ®. Jakiegokolwiek wykorzystywanie wyników itp. w całości lub częściowo jest dozwolone TYLKO za wydaną przed publikacją wyraźną pisemną zgodą Zarządu firmy AV-Comparatives e.V. AV-Comparatives e.V. oraz ich wybrani przedstawiciele wykonujący testy nie mogą być odpowiedzialni za zniszczenie lub stratę, które mogłyby mieć miejsce jako następstwo lub w związku z wykorzystaniem informacji zamieszczonych w tym dokumencie. Szczególnie zadbaliśmy o zapewnienie poprawności podstawowych danych, jednakże nie możemy brać odpowiedzialności za poprawność wyników testów przeprowadzonych przez któregokolwiek z przedstawicieli AV-Comparatives e.V. Nie gwarantujemy poprawności, kompletności ani przydatności w przypadkach szczególnych jakiegokolwiek informacji bądź treści przedstawionej w dowolnym miejscu dokumentu. Nikt inny, kto brał udział w tworzeniu, przedstawianiu czy dostarczaniu wyników testów, nie będzie odpowiedzialny za żadne wtórne, specjalne czy pośrednie zniszczenie lub utratę zysków związane z wykorzystaniem lub niemożnością wykorzystania usług dostępnych na stronie internetowej, dokumentów testowych czy jakichkolwiek powiązanych z nimi danych. AV-Comparatives e.V. jest organizacją typu non-profit zarejestrowaną w Austrii.

Więcej informacji na temat AV-Comparatives oraz wdrożonych metodologii testowania można znaleźć na naszej stronie internetowej.

AV-Comparatives e.V. (Maj 2009)