

G Data ClientSecurity Business 10

Specyfikacja techniczna oprogramowania antywirusowego chroniącego stacje robocze i serwery plików

1. Wymagania: Windows 7 (tylko klient), Vista, XP SP2, Server 2008, 2003 Server, 2000 SP4 (tylko klient), Linux (tylko klient) , od 256 MB RAM.
2. Wsparcie dla 32- i 64-bitowych wersji systemu Windows.
3. Interfejsy programu, pomoce i podręczniki w języku polskim.
4. Pomoc techniczna w języku polskim.

Ochrona antywirusowa i antyspamowa

5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
7. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
8. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
9. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.
10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11. 2 niezależne skanery antywirusowe z 2 niezależnymi bazami sygnatur wirusów wykorzystywane przez monitor antywirusowy oraz do jednorazowego i periodycznego skanowania plików.
12. Możliwość konfiguracji programu do pracy z jednym (dowolnym) skanerem lub dwoma skanerami jednocześnie.
13. Dodatkowy i niezależny od skanerów plików trzeci skaner poczty niewymagający aktualizacji (kontrola antywirusowa i antyspamowa na serwerach zewnętrznych).
14. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
15. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
16. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
17. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
18. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
19. Możliwość skanowania dysków sieciowych i dysków przenośnych.
20. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
21. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

23. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
24. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
25. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
26. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
27. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
28. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
29. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
32. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
33. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
34. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
35. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
36. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
37. Aktualizacja dostępna z bezpośrednio Internetu, lub offline – z pliku pobranego zewnętrznie.
38. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
39. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
40. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
41. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, antyspam, skaner HTTP).
42. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.

Osobista zapora połączeń sieciowych

43. Zapora działająca domyślnie trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika
44. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.

45. Możliwość wyboru jednej z 4 akcji w trakcie tworzenia reguł w trybie interaktywnym: akceptuj, blokuje, akceptuj teraz, blokuje teraz.
46. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnej ilości połączeń.
47. Wbudowany system IDS.
48. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
49. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych

Zdalne administrowanie ochroną

50. Centralna instalacja i zarządzanie wszystkimi programami na stacjach roboczych i serwerach Windows.
51. Zdalna instalacja oprogramowania klienckiego na stacjach roboczych Windows.
52. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
53. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
54. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
55. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
56. Możliwość zdalnego zarządzania serwerem przez przeglądarki Internetowe (z sieci lokalnej i spoza niej).
57. Szyfrowanie komunikacji między serwerem zarządzającym a klientami (SSL).
58. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
59. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
60. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
61. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
62. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
63. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
64. Możliwość generowania raportów w formacie XML.
65. Możliwość przeglądania statystyk ochrony antywirusowej w postaci graficznych wykresów z możliwością eksportu wykresów do różnych formatów grafiki.