

## **Antywirus – stacje robocze 45 sztuk**

### **Specyfikacja produktowa oprogramowania antywirusowego chroniącego stacje robocze**

1. Pełne wsparcie dla systemów Windows: 11, 10, 8.1, 7 (min. SP1).
2. Pełne wsparcie dla systemów Windows Server: 2022, 2019, 2016, 2012 R2, 2012.
3. Wsparcie dla systemów Windows XP SP3 32-bit, Vista (min. SP1), 8, Windows Server 2008 R2, 2008, 2003, Linux 32/64-bit, OS X (tylko klient).
4. Interfejsy programu, pomoce i podręczniki w języku polskim.
5. Pomoc techniczna w języku polskim.
6. Ochrona przed zagrożeniami typu 0-day na poziomie co najmniej 99,5% we wszystkich testach niezależnej organizacji AV-TEST przeprowadzonych w roku 2024.
7. Wskaźnik Malware Protection Rate na poziomie co najmniej 98,8% we wszystkich testach Business Security Test niezależnej organizacji AV-Comparatives przeprowadzonych w roku 2024.

### **Ochrona antywirusowa**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
4. Moduł do ochrony przed exploitami (ataki 0-day).
5. Moduł do ochrony przed ransomware.
6. Mechanizm ochrony przed zamaskowanym złośliwym kodem wykorzystujący sieć neuronową opartą o algorytmy adaptacyjne.
7. Moduł ochrony proaktywnej, oparty na teorii grafów, uczący się zachowania systemu operacyjnego i wykrywający podejrzane działania.
8. Moduł wykrywający złośliwy kod w skryptach Powershell, WScript, CScript, Mshta oraz elementach aktywnych w programach MS Office.
9. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
10. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.
11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Dwa niezależne skanery antywirusowe (nie heurystyczne!) z dwoma niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
13. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
14. Dodatkowy i niezależny od skanerów plików, trzeci skaner poczty oparty o technologię cloud security.
15. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
16. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
17. 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, rodzaj plików do skanowania, priorytet skanowania).
18. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

19. Technologia zapobiegająca powtórному 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.
20. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
21. Możliwość skanowania dysków sieciowych i dysków przenośnych.
22. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
23. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
24. 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.
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 odebranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
29. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
31. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
32. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
33. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
34. Ochrona przed stronami phishingowymi działającymi przy użyciu protokołów HTTP i HTTPS.
35. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
36. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
37. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
38. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
39. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
40. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
43. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).

44. Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
45. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
46. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznowiane automatycznie, podczas gdy nie jest on używany.
47. Ochrona przed urządzeniami podszywającymi się pod klawiatury USB.
48. Agentowa ochrona maszyn wirtualnych wykrywająca znane i nieznane zagrożenia przy użyciu zdalnego serwera skanowania oraz technologii proaktywnych.
49. Agent ochrony maszyn wirtualnych delegujący zlecenie skanowania do wirtualnego serwera skanowania.
50. Wirtualny serwer skanowania dostarczony w formie gotowego obrazu (appliance) dla środowisk HyperV oraz VMware.

### **Zdalne administrowanie ochroną**

1. Integracja z Active Directory – import kont komputerów i jednostek organizacyjnych.
2. Zarządzanie urządzeniami z systemem Android i iOS.
3. Przenośna konsola administracyjna pobierająca interfejs zgodny z serwerem zarządzającym.
4. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.
5. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i serwerach Windows.
6. Zdalna instalacja i centralne zarządzanie klientami Linux / OS X.
7. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
8. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
9. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
10. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
11. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
12. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
13. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
14. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
15. Możliwość zarządzania ochroną sieci wielu usługobiorców z poziomu jednej instancji serwera zarządzającego.
16. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
17. Możliwość zdalnego uruchomienia skanowania antywirusowego wybranych stacji roboczych.
18. Możliwość pobrania z kwarantanny pliku w postaci zaszyfrowanej.
19. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
20. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (nazwa, wersja, producent, data instalacji).

21. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.
22. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku/partycji systemowej).
23. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
24. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
25. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
26. 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).
27. Możliwość generowania raportów w formacie XML.
28. Możliwość komentowania raportów związanych z bezpieczeństwem.
29. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.
30. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.
31. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej.
32. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.
33. Możliwość dynamicznego grupowania stacji na podstawie parametrów: nazwa komputera, adres IP, brama domyślna, nazwa domeny.
34. Raportowanie nieudanych prób logowania do serwera zarządzającego.
35. Monitorowanie stanu działania stacji pomimo nieaktywnej ochrony antywirusowej.
36. Możliwość integracji z systemami SIEM - Security Information and Event Management.
37. Rejestrowanie zdarzeń bezpieczeństwa w dziennikach zdarzeń systemu Windows.
38. Szczegółowe informacje analityczne zdarzeń dotyczących bezpieczeństwa (w tym SHA256, ostatni dostęp i próba zapisu do pliku, właściciel, nazwa procesu wywołującego).

### **Urządzenia mobilne (Mobile Device Management)**

1. Zintegrowany moduł Mobile Device Management do obsługi urządzeń mobilnych.
2. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli oraz interfejsu www.
3. Pełne wsparcie dla systemów Android (wersja 7 i wzwyż) oraz iOS (wersja 9 i wzwyż)
4. Możliwość zdalnej instalacji i konfiguracji ochrony na urządzeniach z systemem Android.
5. Zarządzanie profilem zabezpieczeń na urządzeniach z systemem iOS.
6. Klient ochrony na urządzenia Android dostępny do pobrania z poziomu Google Play.
7. Możliwość skonfigurowania w urządzeniach z systemem Android: aktualizacji sygnatur, ochrony aplikacji, ochrony przeglądarek internetowych, ochrony karty SIM, domyślnej sieci WiFi, blokady aplikacji.
8. Możliwość skonfigurowania w urządzeniach z systemem iOS: ustawień kodu, ograniczenia funkcjonalności, ograniczeń aplikacji, ograniczeń treści.
9. Konfigurowanie urządzeń poprzez wprowadzanie profili zabezpieczeń zdefiniowanych przez administratora.

10. Moduł antykradzieżowy pozwalający przynajmniej: zlokalizować urządzenie, zablokować urządzenie, przywrócić do domyślnych ustawień.
11. Interfejs podpowiadający zalecenia bezpieczeństwa dotyczące urządzeń mobilnych.
12. Możliwość wysłania żądania usunięcia zainfekowanej aplikacji do klienta.
13. Moduł raportowania pozwalający na skontrolowanie stanu zabezpieczeń urządzeń mobilnych.
14. Interfejs klienta Android pozwalający na przeskanowanie urządzenia pod kątem zagrożeń.

### **Raporty**

1. Możliwość utworzenia raportów statusu ochrony sieci.
2. Możliwość generowania raportów w przynajmniej 3 językach.
3. Możliwość wysyłania raportów z określonym interwałem.
4. Możliwość wysyłania jednego raportu na różne adresy mailowe lub grupy adresów.
5. Możliwość zdefiniowania przynajmniej 15 różnych typów informacji dotyczących statusu ochrony oraz różnych form ich przedstawienia (tabele, wykresy) w pojedynczym raporcie.

### **Osobista zapora połączeń sieciowych**

1. W pełni zdalna instalacja, zdalne zarządzanie wszystkimi funkcjami zapory i zdalna deinstalacja.
2. Zapora działająca domyślnie w trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika.
3. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
4. Możliwość interakcji między użytkownikiem a administratorem w celu dostosowania zestawu reguł.
5. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnych grup użytkowników.
6. Wbudowany system IDS.
7. Możliwość pracy w trybie offsite po odłączeniu od sieci przedsiębiorstwa.
8. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
9. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych.
10. Automatyczne wysyłanie powiadomień o zablokowaniu aktywności sieciowej na wskazany adres mailowy.
11. Import/eksport reguł/zestawów reguł zapory na stacji roboczej.

### **Zdalne zarządzanie wydajnością i czasem pracowników (PolicyManager)**

1. Wszystkie obostrzenia modułu można zastosować zarówno wobec użytkowników z ograniczonymi kontami Windows, jak i administratorów.
2. Kontrola aplikacji umożliwiająca blokowanie lub zezwalanie na stosowanie konkretnych programów, folderów i plików. Opcja zablokowania pliku w konkretnej wersji, o danej sumie kontrolnej oraz podpisanego cyfrowo przez wskazanego producenta.
3. Kontrola urządzeń pozwalająca na zarządzanie dostępem do napędów CD/DVD/BD, pendrive'ów, dysków, kamer USB oraz urządzeń Windows Portable Devices, a także tradycyjnych stacji dyskiety. Możliwe jest zablokowanie urządzenia a także ustawienie dostępu tylko do odczytu.
4. Możliwość wykluczenia urządzeń na podstawie ich numeru ID i nadanie im pełnych uprawnień lub tylko do odczytu.

5. W przypadku wykluczeń urządzeń możliwe jest napisanie odpowiedniego komentarza dla danego wyjątku.
6. Kontrola treści internetowych umożliwiającą zablokowanie/odblokowanie użytkownikom stron internetowych z konkretnych kategorii. Rozbudowana lista aktualizowana jest przez Internet.
7. Biała i czarna lista stron internetowych stosowana bez względu na przypisaną im kategorię treści.
8. Kontrola czasu spędzanego w Internecie. Możliwość precyzyjnego określenia w jakich godzinach jakiego dnia użytkownik może przeglądać treści internetowe. Dodatkowo można określić dzienny, tygodniowy oraz miesięczny limit czasu przeznaczony do korzystania ze stron internetowych.
9. Po zablokowaniu aplikacji, urządzenia lub strony internetowej użytkownik może zażądać udostępnienia zablokowanego zasobu wprost z okna z komunikatem o blokadzie.
10. Administrator ma możliwość odblokowania zasobu z poziomu raportu konsoli zarządzającej utworzonego automatycznie po zaznaczeniu przez użytkownika opcji zażądania dostępu do zablokowanego zasobu.
11. Automatyczne wysyłanie powiadomień o zablokowaniu danego zasobu na wskazany adres mailowy.