

Warunki równoważności

Minimalne warunki równoważności:

- Konsola centralnego zarządzania umożliwiająca:
 - o stosowanie firmowych zasad zabezpieczeń, które nie mogą zostać ominięte przez użytkowników końcowych
 - o generowanie szczegółowych raportów internetowych umożliwiających monitorowanie stanu całej zarządzanej sieci
 - o scentralizowane zarządzanie instalacjami, aktualizacjami, uaktualnieniami i monitorowaniem
 - o szybkie zarządzanie zasadami w obrębie całej organizacji
 - o zarządzanie oprogramowaniem antywirusowym i ochroną antyspieszającą, ochroną przed programami typu rootkit, systemami monitorowania zachowań, zaporami chroniącymi stacje robocze, zabezpieczeniami przed włamaniami oraz kontrolą aplikacji na stacjach roboczych i komputerach przenośnych, zarządzanie ochroną przed spamem
 - o zdalne zarządzanie lokalnymi kwarantannami
 - o możliwość instalacji zdalnej
 - o szczegółowe raporty graficzne dotyczące alertów zabezpieczeń i stanu zabezpieczeń sieci
 - o łatwe dodawanie klientów — bez potrzeby ręcznego importowania poszczególnych komputerów
 - o wydajna technologia aktualizowania baz systemu wirusów
- Automatyczna ochrona stacji roboczych i serwerów w czasie rzeczywistym przed wirusami, oprogramowaniem szpiegującym, robakami i końmi trojańskimi.
- Funkcja ochrony przeglądania informuje, które witryny internetowe są bezpieczne, i blokuje szkodliwe witryny
- Funkcja osłony luk uniemożliwia przestępcom uzyskiwanie dostępu do komputerów za pośrednictwem luk w zabezpieczeniach oprogramowania.
- Ochrona przed nieznanymi zagrożeniami zmieniającymi ustawienia systemowe, przechwytyjącymi przeglądarki i podstawiającymi kod.
- Skanowanie w poszukiwaniu programów typu rootkit i ich usuwanie
- Skanowanie ruchu POP3, SMTP i IMAP4 poczty e-mail.
- Ochrona przed oprogramowaniem szpiegującym zatrzymująca oprogramowanie reklamowe i szpiegujące przy użyciu skanera działającego w czasie rzeczywistym.
- Kwarantanna sieciowa zapewniająca odpowiedni poziom ochrony zdalnych komputerów przenośnych łączących się z siecią firmową spoza biura przed przyznaniem im dostępu.
- Niewidoczne, automatyczne aktualizacje ochrony antywirusowej i antyspieszającej, dostarczane kilka razy dziennie
- Zgodność z rozwiązaniem Microsoft DirectAccess i Microsoft Network Access Protection (NAP)
- Automatycznie generowane raporty
- Skanowanie zaplanowane i na żądanie
- Funkcja wykluczania zaufanych procesów ze skanowania w czasie rzeczywistym
- Zgodność z rozwiązaniami VMware i Citrix XenApp
- Funkcjonalności dla Microsoft Exchange 2010:
- Skanowanie w czasie rzeczywistym wiadomości przychodzących i wychodzących
- Proaktywna ochrona przed nieznanymi zagrożeniami
- Wydajny mechanizm ochrony przed spamem

Minimalny wykaz dedykowanych wersji dla:

- Systemów serwerowych Citrix
- Systemów serwerowych Windows (Windows Server 2003 I 2003 R2, Windows Server 2008 I 2008 R2) oraz wszystkich nowych wprowadzanych w okresie ochrony
- Systemów operacyjnych stacji roboczych Windows (XP, Vista, 7) oraz wszystkich nowych wprowadzanych w okresie ochrony
- Microsoft Exchange 2010 oraz wszystkich nowych wprowadzanych w okresie ochrony

Elementy uzupełniające:

- Konsola centralnego zarządzania z bazą sygnatur