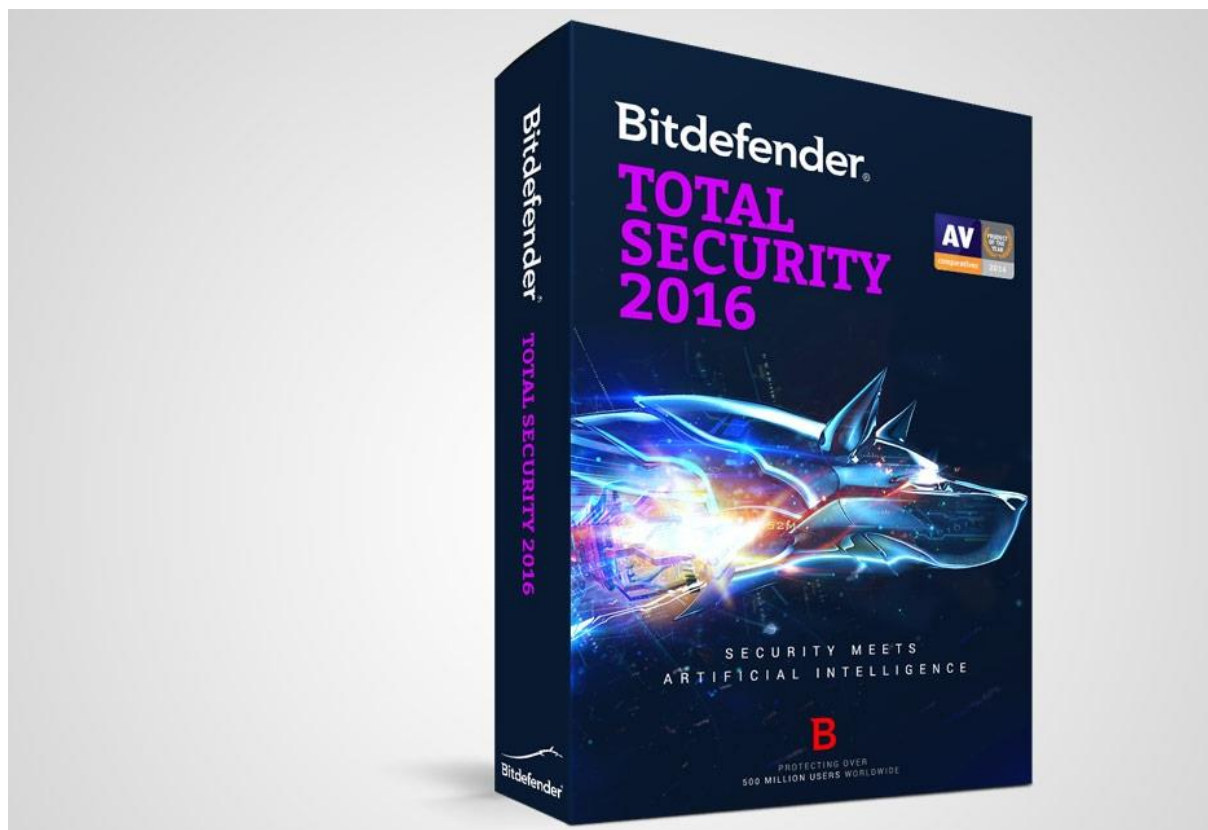


Bitdefender Total Security 2016 - rewelacyjny antywirus w dobrej cenie

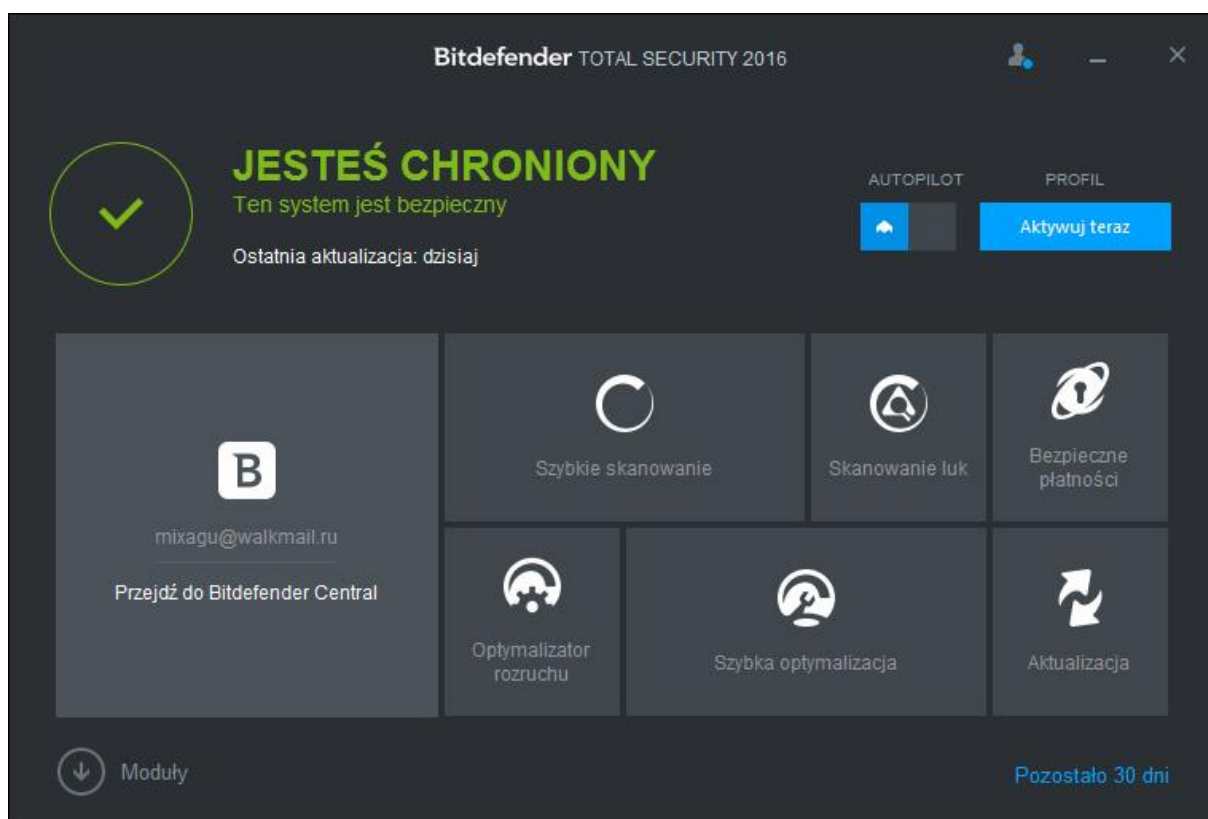
Bitdefender Total Security 2016 to na pewno jeden z najlepszych, jeśli nie najlepszy pakiet zabezpieczający komputer przed złośliwym oprogramowaniem.



Oprogramowania antywirusowego tworzonego nieustannie od 2007 roku przez producenta [Bitdefender](#) (a wcześniej pod nadzorem innych spółek) nie trzeba nikomu przedstawiać. Całe lata współpracy rumuńskich inżynierów z zespołami bezpieczeństwa, specjalistami do walki z cyberzagrożeniami, ludźmi zajmującymi się analizą kodu oraz analizą incydentów i specjalistami od cyberbezpieczeń sprawiły, że aplikacje te mogą dzisiaj pochwalić się najskuteczniejszym silnikiem antywirusowym spośród konkurencyjnych produktów. I nie są to czcze przechwałki.

Bitdefender niemal we wszystkich testach niezależnych laboratoriów zdobywa wyróżnienia – nie tylko pod względem jakości ochrony, ale także niewielkiego wpływu na wydajność chronionego komputera.

Premiera recenzowanego Bitdefender Total Security 2016 miała miejsce w ubiegłym roku. Osoby, które chciałyby się cieszyć komunikatami oraz interfejsem programu w języku polskim, mogą pobrać aplikację bezpośrednio ze strony polskiego dystrybutora (Marken Systemy Antywirusowe).

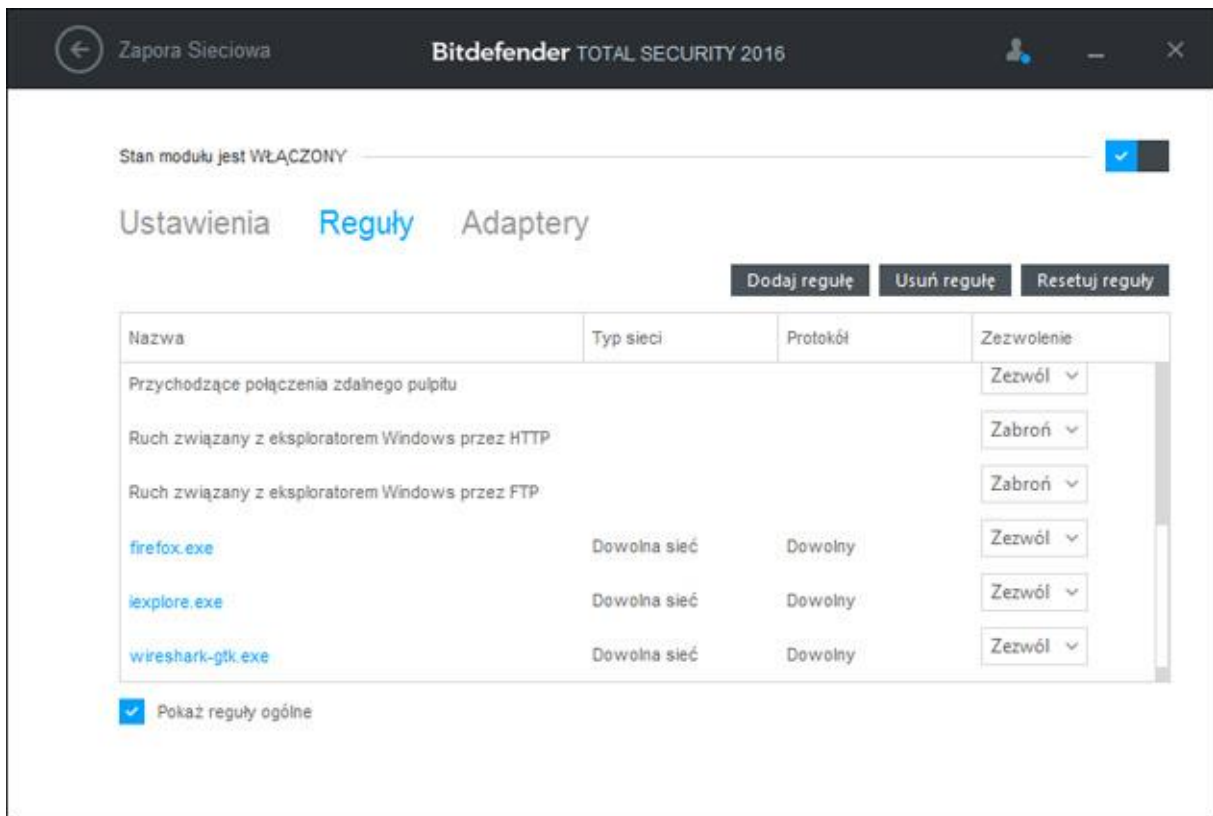


Zatrzymując się na chwilę przy interfejsie należy nadmienić, iż w ostatnich latach dostawcy rozwiązań antywirusowych zbyt wiele uwagi przywiązują do panujących trendów, a wcześniej trendów, które były kreowane przez Microsoft i ich kafelkowe Windows 8. W przypadku Bitdefendera niewiele zmieniło się od wersji z poprzedniego roku - właściwie to czemu miałyby? Za to producent postanowił:

1. Pośrednio odebrać użytkownikom kontrolę nad dwukierunkowym firewallem zintegrowanym z aplikacją Bitdefender Internet Security 2016 oraz Bitdefender Total Security 2016 rezygnując z trybu interaktywnego.

Tłumacząc to na bardziej zrozumiały język – nie jest możliwa konfiguracja zapory internetowej w taki sposób, aby podczas próby łączenia się dowolnej aplikacji ze światem zewnętrznym, antywirus proponował użytkownikowi komputera stworzenie reguły sieciowej poprzez wyświetlenie odpowiedniego komunikatu czekając na podjęcie decyzji.

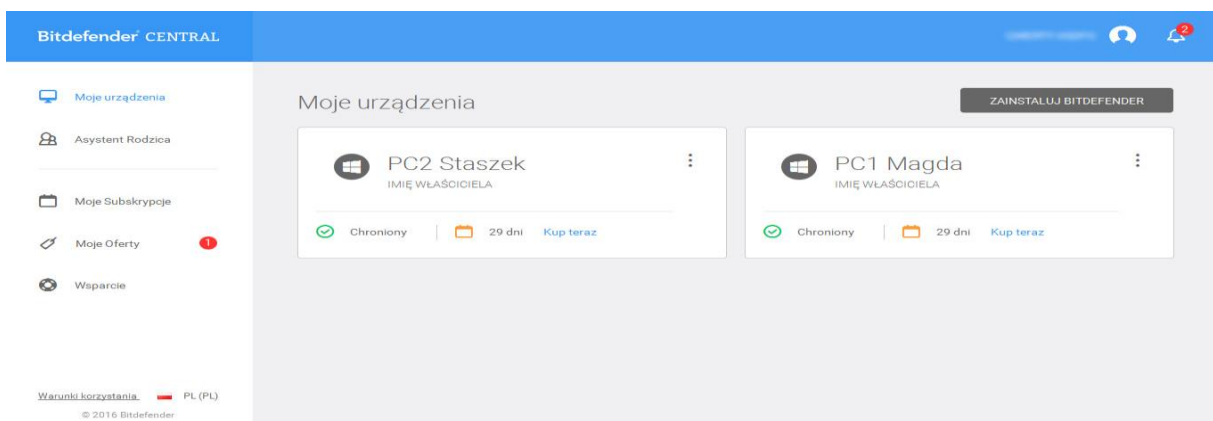
Oczywiście wyjątki dla programów (np. przeglądarek, klientów poczty, gier, procesów systemowych), a także protokołów czy nawet portów są dostępne z poziomu interfejsu graficznego w sekcji „zapora sieciowa->reguły”. Problem jednak w tym, że to Bitdefender automatycznie podejmuje decyzję, „czy i kiedy” zezwolić na połączenie z internetem, co nie każdemu może się podobać.



Mając na uwadze automatyzację Bitdefendera (funkcja autopilot), która de facto zawsze była dużym plusem tego programu – podejście producenta do firewall'u nie jest takie złe, na jakie wygląda. Na pewno docenią to użytkownicy, dla których antywirus jest złem koniecznym, aplikacją typu „zainstaluj-zapomnij”.

Jednak zupełnie inaczej odbierają to osoby, które od oprogramowania antywirusowego wymagają czegoś więcej niż tylko ładnego GUI. Użytkownicy, którzy na firewallu programowym na bieżąco dostosowują poszczególne składniki systemu i programów zainstalowanych w systemie do własnych preferencji poczują się bezpieczniej w cyfrowym świecie, który nieustannie prowokuje złodziei i przestępców.

2. Wymusić aktywację antywirusa (nawet dla wersji trial) logując się do Bitdefender Central.



Podejście takie znalazło zarówno przeciwników jak i zwolenników. Tej pierwszej grupie nie podoba się integracja antywirusa z poniekąd zewnętrzną usługą, aczkolwiek nadal zlokalizowaną na serwerach producenta Bitdefender.

Z kolei druga grupa osób nie ma nic przeciwko jednej internetowej konsoli, w której odnajduje swoje wszystkie klucze licencyjne i chronione urządzenia, które mogą być zdalnie zarządzane (dostępne są podstawowe komendy skanowania, optymalizacji komputera, uruchomienia skanera podatności). Dla urządzeń przenośnych (laptopów, smartfony, tabletów) możliwe jest wydanie polecenia zdalnej lokalizacji.

Bitdefender Central stanowi nadrzędny punkt, w którym przechowywane są wszystkie informacje o urządzeniach (Windows, Mac, Android) i kupionych lub wygranych w konkursach subskrypcjach na oprogramowanie Bitdefender. Użytkownik, który najpierw pobierze wersję instalacyjną antywirusa ze strony dystrybutora, po jego zainstalowaniu będzie proszony o zalogowanie się (przy pomocy jednego z kont FB, G+, Microsoft) lub utworzenie odrębnego w Bitdefender Central. Jest to niezbędny krok, aby w ogóle aktywować ochronę antywirusową.

Jednak jest on do obejścia i należy go odwrócić. Jeszcze przez instalacją tworzymy konto w portalu central.bitdefender.com i ze swojej web konsoli pobieramy instalator antywirusa Bitdefender. W ten sposób zainstalowany antywirus automatycznie zgłosi urządzenie do Bitdefender Central.

Architektura ochrony antywirusów Bitdefender

Bitdefender przez wiele lat pracował na wyniki osiągnięte nie tylko w testach, które co do zasady mają na celu przedstawić faktyczną skuteczność walki ze złośliwym oprogramowaniem. Rumuni swoje miejsce w szeregu wypracowali popularnością, która nie bez kozery odzwierciedla przecież stosunek producenta do klienta, jakość usługi i cenę produktu. Klientów Bitdefendera jest już ponad 500 milionów na całym świecie. Czy jakkolwiek inny producent może się pochwalić taką liczbą?

Dla porównania, bardzo popularny u nas w Polsce antywirus Comodo – skuteczny, stabilny soft, ze wspaniałą automatyczną piaskownicą, która nieznane (na podstawie sygnatur i reputacji w chmurze) pliki i aplikacje automatycznie odizolowuje od systemu operacyjnego, zdobył do tej pory niecałe 100 milionów użytkowników. Wynik również wyśmienity, warty odnotowania, jednak Comodo musi swoje wysiłki zwiększyć aż pięciokrotnie.

Skuteczność ochrony w najnowszym pakiecie Bitdefender Total Security 2016 to nie tylko liczby i statystyki. To także rozwijana już od wielu lat technologia proaktywnego wykrywania zagrożeń, która oparta o analizę behawioralną (B-HAVE) pozwoliła uniezależnić silnik antywirusowy od detekcji wirusów identyfikowanych wyłącznie na podstawie opracowanych sygnatur statycznych lub generycznych.

Nieznany, potencjalnie niebezpieczny wykonywalny plik (exe, com, dll, sys, bat) jest uruchamiany w wirtualnym środowisku, gdzie sprawdzane jest jego bezpieczeństwo: B-HAVE uruchamiając aplikacje opóźnia ich start aż do zasymulowania zachowania programu. W przypadku, kiedy nie zostaną wykryte żadne złośliwe działania, aplikacja

opuszcza środowisko sandbox i uruchamia się normalnie. Jeżeli podejrzane zachowanie zostanie wykryte, B-HAVE automatycznie poddaje zagrożenie kwarantannie lub go usuwa.

Drugą linię obrony stanowi technologia Active Virus Control, która w synergicznym działaniu z B-HAVE stale monitoruje procesy uruchomione w systemie i sprawdza każdą anomalię przydzielając jej określoną ilość punktów. Po osiągnięciu danego progu (tzw. współczynnik zagrożenia), proces jest uznawany za szkodliwy. W ten właśnie sposób działa większość mechanizmów antyspamowych, które zintegrowane są z antywirusami - wykorzystują algorytm Bayesa, skanują nagłówki wiadomości, łączniki, treść oraz weryfikują adresy IP nadawcy, a także adresy URL z tymi w bazie danych serwerów RBL i SURBL.

Oczywiście to jeszcze nie wszystko. Bitdefender opracował technologię Photon, której zadaniem jest poprawa szybkości i wydajności komputera poprzez dostosowanie priorytetu działania antywirusa do unikalnej konfiguracji sprzętowej.

Producent stworzył także bazujący na chmurze obliczeniowej mechanizm maszynowego uczenia się – algorytm, który potrafi zidentyfikować nowe, nieznane jeszcze producentowi zagrożenia, czy złośliwe adresy URL. Zgromadzone w jednej centralnej bazie dane są automatycznie przetwarzane, by uzyskać stosunkowo dużo charakterystycznych dla wirusów danych, które mogą być wykorzystane do przewidywania przyszłych zagrożeń.

Ale czy tylko z tego znany jest Bitdefender? Od zawsze programy rumuńskiego producenta świetnie radziły sobie ze stronami internetowymi, które dystrybuowały złośliwą zawartość. Plugin o nazwie Bitdefender TrafficLight polecam każdemu użytkownikowi, który chciałby solidnie zabezpieczyć się przed witrynami typu phishing oraz stronami ze złośliwymi skryptami Java, JavaScript, iFrame powszechnie stosowanymi w kampaniach malvertising.

Co Bitdefender Total Security 2016 oferuje poza kompleksową ochroną?

Użytkownik oprócz ochrony przed całym spektrum zagrożeń otrzymuje dodatkowo:

- **Środowisko Bitdefender SafePay** (Bezpieczne płatności), które powinno być wykorzystane do robienia zakupów w sieci i przelewów internetowych (SafePay jest dostępny za darmo dla każdego użytkownika systemu Windows).
- **Bitdefender Wallet** – bezpieczny portfel, sejf – lub jeszcze inaczej – menadżer haseł, kodów, pinów, innych ciągów znaków, które mogą być zapamiętane w antywirusie i zaszyfrowane.
- **Tune-Up** – dzisiejsze pakiety Internet Security lub te bardziej rozbudowane Total Security / Total Protection już od dawna łączą ochronę z wydajnością systemów. Tune-up może stanowić alternatywę dla popularnego CCleanera.

- **File Shredder** – funkcja niszcarki plików, która według producenta nadpisuje usuwane dane określoną ilość razy i uniemożliwia odzyskanie ich nawet technikami stosowanymi w informatyce śledczej (ang. computer forensics).
- **Battery Mode** – moduł, który wstrzymuje instalację i pobieranie aktualizacji systemu Windows, kiedy urządzenie pracuje na baterii.
- **Vulnerability Scanner** – niezwykle przydatny w dzisiejszych czasach skaner „podatności”, a właściwie narzędzie, które wyszukuje niezainstalowane aktualizacje systemu z Windows Update oraz stare wersje programów trzecich, takich jak przeglądarki, Java, Flash, itp., niwelując ryzyko ataków o te wektory.
- **Kontrola rodzicielska** – niezwykle rozbudowana funkcjonalność (dostępna z poziomu Bitdefender Central), która wymaga odrębnej recenzji. Rodzice otrzymują multum funkcji, które pomagają kontrolować, monitorować, blokować niewłaściwe treści dla dziecka. Przy czym wszystko to dostępne jest oczywiście w języku polskim, a sama konfiguracja jest banalnie łatwa.

A jak Bitdefender Total Security 2016 wypada w testach?

Według niezależnych laboratoriów takich jak AV-Test oraz AV-Comparatives, a także Virus Bulletin - jest dobrze, jeśli nie rzec - bardzo dobrze. Rzućmy okiem na najnowszy test niemieckiego labu AV-Test. Pomimo, że testowano tutaj wersję Bitdefender Internet Security 2016, na różnice w stosunku do Bitdefender Total Security 2016 składają się dodatkowe narzędzia.

	November	December	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 140 samples used	100%	100%	97.1%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 14,658 samples used	99.9%	100%	99.7%
Protection Score ●●●●●● 6.0/6.0			

Testy AV-Test (ich pełna metodologia i metodyka została przedstawiona przez polski serwis AVLab) publikowane są co dwa miesiące i są podzielone na dwie części. Pierwsza odzwierciedla skuteczność ochrony przez zagrożeniami 0-day, a więc takimi, które nie są znane producentowi lub są, ale nie opracowano metody na ich wykrycie. Bitdefender w tych testach zawsze wypada rewelacyjnie. Z kolei druga część testów ochrony odzwierciedla detekcję kilkunastu lub kilkudziesięciu tysięcy (w zależności od miesiąca) skompletowanych na 4 tygodnie przed testem próbek.

AV-Test odwzorowuje także wydajność testowanych pakietów Internet Security, jednak nie sprawdza apetytu na procesor i RAM, a szybkość wczytywania stron internetowych, pobierania programów, instalowania i uruchamiania aplikacji oraz

kopiowania danych. Także i tutaj Bitdefender Internet Security niemal zawsze zdobywa 6 punktów na 6 możliwych.

Ostatnia część testu to „użyteczność”. Tłumacząc to na język polski – podatność antywirusa na fałszywe alarmy podczas otwierania bezpiecznych stron internetowych, ilość false positive podczas skanowania ponad miliona zaufanych plików oraz liczba FP komunikatów ostrzegających i blokujących instalowane i uruchamiane bezpieczne aplikacje.

Wydajność i testy AV-Comparatives

Wiele osób zapomina lub nie wie, że lepszą wydajność antywirusa można uzyskać w bardzo prosty sposób. Metoda ta jest sprawdzona, potwierdzona przez producentów antywirusów, aczkolwiek nie we wszystkich przypadkach skuteczna. Wiele zależy od konfiguracji sprzętowej, którą jak to mówią – (czasami) „nie przeskoczysz”.

Antywirus jest specyficzną aplikacją, która non-stop monitoruje, odczytuje, zapisuje, skanuje pliki, procesy, strony internetowe i ruch sieciowy. Aby zwiększyć lokalną wydajność wystarczy tylko uruchomić kompleksowe, pełne skanowanie wszystkich dysków (całego komputera), po to, aby specjalne algorytmy odpowiedzialne za skanowanie plików nie weryfikowały tych już bezpiecznych, umieszczonych na białej liście; lub by były skanowane tylko wtedy, kiedy zostaną ponownie zmodyfikowane lub otworzone przez proces / użytkownika. Nie zawsze operacja ta jest efektywna, jednak powinno się ją zawsze wykonać po zainstalowaniu antywirusa.

Metodologia testów wydajnościowych w labie AV-Comparatives jest bardzo podobna do tej wykorzystywanej przez AV-Test. Jednak Austriacy stosują dodatkowo benchmark PCMark Home Edition 8 do uzyskania ogólnego stanu wydajności. Bitdefender Internet Security 2016 na 100 możliwych punktów zdobył 99,5.

Kilka słów na koniec

Analizując całą recenzję od końca zatrzymajmy się na chwilę przy testach. Testy są potrzebne, nie da się tego ukryć. Są ważną wykładnią wyboru antywirusa. Dlatego tak samo, jak zakup nowego procesora, urządzenia wielofunkcyjnego, samochodu, telewizora lub kołyski dla dziecka, powinien być przemyślany, a na końcową decyzję winny składać się dokładnie wyselekcjonowane argumenty. W przeciwieństwie do innych „produktów”, wszystkie płatne antywirusy oferują bezpłatny okres próbny, który może być wykorzystany do dokładnego zapoznania się z programem, funkcjami i możliwościami.

Adrian Ścibor, AVLab.pl - dla serwisu benchmark.pl

Źródło: http://www.benchmark.pl/testy_i_recenzje/bitdefender-total-security-2016-test.html