AV-LAB

THE INDEPENDENT ANTIVIRUS TESTS

Test serwera bezpieczeństwa Bitdefender GravityZone Virtual Appliance

Data testu:
17.05.2016

Spis treści

Wprowadzenie

Dotychczas, programy, które poddawaliśmy testom w większym lub w mniejszym stopniu wpływały na wydajność systemu operacyjnego. Niektórzy dostawcy oprogramowania antywirusowego dla firm, podchodzą do kwestii bezpieczeństwa tradycyjnie. Inni powoli rezygnują lub przynajmniej ograniczają detekcję zagrożeń z wykorzystaniem opracowanych sygnatur statycznych bądź generycznych przenosząc je do swojego centrum danych, z kolei niektórzy z nich łączą te dwie metody stawiając na tradycję, która wspierana jest rozwiązaniem hybrydowym.

Produkt GravityZone został opracowany z myślą o bezinwazyjnej ochronie środowisk wirtualnych. Daje administratorom niebywałą kontrolę nad techniką skanowania, z której program antywirusowy będzie korzystał w czasie rzeczywistym zabezpieczając wirtualne i tradycyjne środowiska robocze przed szkodliwym oprogramowaniem. Ten test ma na celu pokazać różnice w wydajności pomiędzy skanowaniem:

Tradycyjnym (lokalnym), gdzie do wykrywania wirusów stosowane są sygnatury oraz ochrona przez heurystykę.

- Hybrydowym - gdzie łączona jest tradycja z nowoczesnością (sygnatury, heurystyka, chmura).
- Centralnym - za pośrednictwem funkcjonalności serwera bezpieczeństwa - integralnej części konsoli GravityZone instalowanej w sieci lokalnej, odciąża ze skanowania stacje robocze.

Aby na powyższych wariantach skanowania sprawdzić wpływ agenta Bitdefender Endpoint Security Tools na zużycie zasobów sprzętowych wirtualnego systemu Windows 10 Pro x64, skorzystaliśmy z monitora wydajności opracowanego przez firmę Microsoft, który jest integralną częścią systemów z rodziny Windows. W badaniu tym sprawdzono rzeczywiste zapotrzebowanie na czas procesora wyrażony w procentach oraz pamięć RAM - wyłącznie przez procesy agenta. Takie podejście do testów, kiedy pod uwagę nie są brane uruchomione w tym samym czasie inne procesy systemowe i aplikacji trzecich pozwala odseparować zużycie zasobów sprzętowych antywirusa od pozostałych procesów oddając rzeczywiste wymagania.

Metodyka

Host 1 o parametrach - CPU: AMD FX-6300, RAM: 8GB DDR3, SSD: 240SSD pełnił rolę środowiska z wirtualnymi maszynami.

Host 2 o parametrach - CPU: i5 2520M, RAM: 8GB DDR3, SSD: 240SSD pełnił rolę urządzenia wirtualnego Bitdefender GravityZone Virtual Appliance z zainstalowanym serwerem bezpieczeństwa.

Do testu przygotowano trzy maszyny wirtualne o przydzielonych zasobach:

CPU: 2x 3,4GHz
RAM: 2GB DDR3
SSD: 40GB

Metodologia

Przed zainstalowaniem na poszczególnych maszynach wirtualnych agentów Bitdefender Endpoint Security Tools, odpowiednio skonfigurowano pakiet instalacyjny agentów Bitdefender dla systemu Windows. Do ochrony stacji roboczej Windows 10 Pro x64 wykorzystano ustawienia predefiniowane przez producenta.

Tag HTML: Info: Wyróżniamy trzy rodzaje skanowania: lokalne, hybrydowe i centralne. Po więcej szczegółów odsyłamy do artykułu “Bitdefender GravityZone Virtual Appliance dedykowany dla środowisk wirtualnych”.

Poniższe wykresy zostały wykonane przez monitor wydajności, który przez 10 minut w trybie jałowym oraz pod obciążeniem zbierał z interwałem ustawionym na 1 sekundę średnie wyniki zapotrzebowania na pamięć RAM i upływ czasu procesora potrzebnego do prawidłowego funkcjonowania aplikacji Bitdefender Endpoint Security Tools.

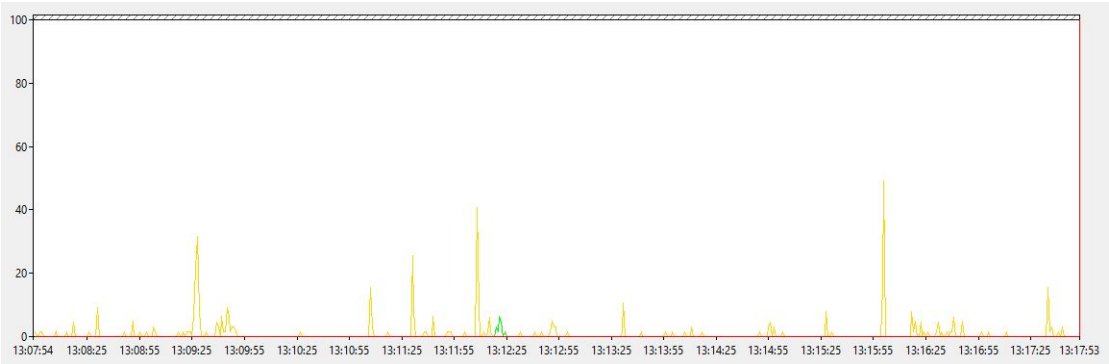
Wykresy zawierają średnie obciążenie RAM i CPU z każdej sekundy badania. Po 10 minutach, działanie monitora wydajnościowego było zatrzymywane. Następnie obliczano średnią wartość z 600 pomiarów z każdej sekundy dla każdego procesu z dokładnością do 1 bajta (dla pamięci RAM). Wynik zamieniano na wartość wyrażoną w megabajtach [MB].

Skanowanie lokalne

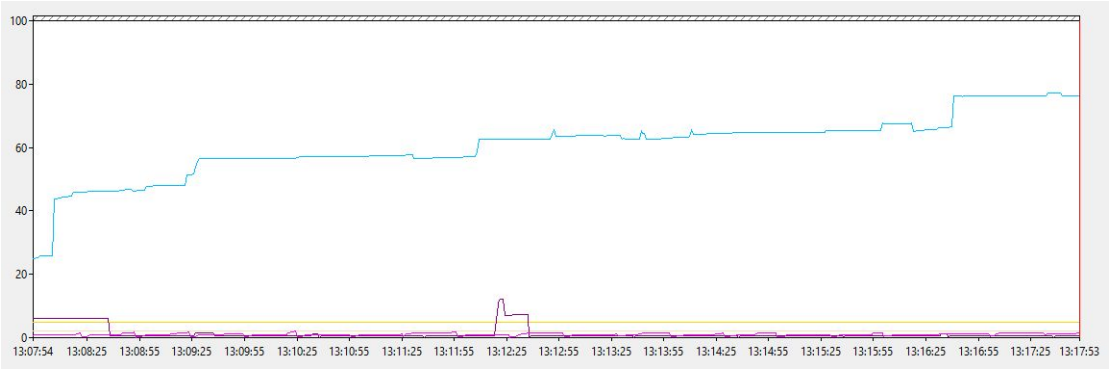
Gdzie - 1: składnik ochrony aktywny, 0: składnik ochrony nieaktywny (ustawienia wg pliku XML z pobranym instalatorem EXE)

```
<features>
<feature action="1" name="FileScan"/>
<feature action="1" name="UserControl"/>
<feature action="1" name="Antiphishing"/>
<feature action="1" name="Firewall"/>
<feature action="0" name="UpdateServer"/>
<feature action="1" name="BehavioralScan"/>
<feature action="1" name="TrafficScan"/>
<feature action="0" name="MailServers"/>
<feature action="1" name="DataLossPrevention"/>
<feature action="1" name="PowerUser"/>
</features>
...
<scanType strVar="ScanType">full</scanType>
```

Tryb jałowy:

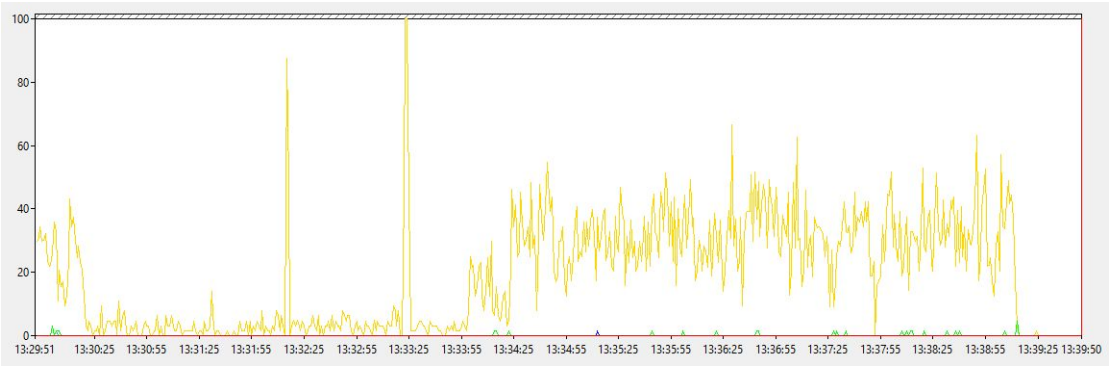


W spoczynku, zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 0,918%. Drugi rdzeń nie był obciążony.

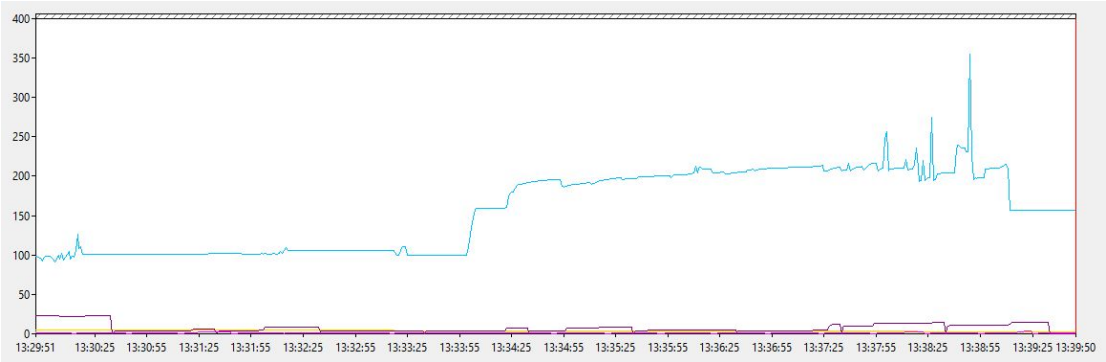


W spoczynku, procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~67MB pamięci RAM.

Skanowanie pełne (wszystkich dysków):



Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 18,121%. Drugi rdzeń nie był obciążony. Maksymalna wartość skokowa osiągnęła ~109%, co oznacza, że jeden rdzeń w tej konkretnej sekundzie został obciążony w 100%, a drugi w około 9%.



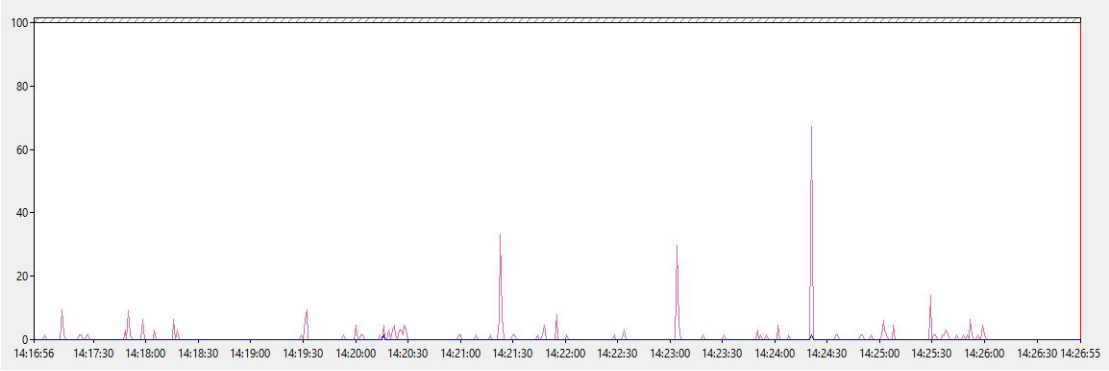
Podczas skanowania, średnio procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~164MB pamięci RAM.

Skanowanie hybrydowe

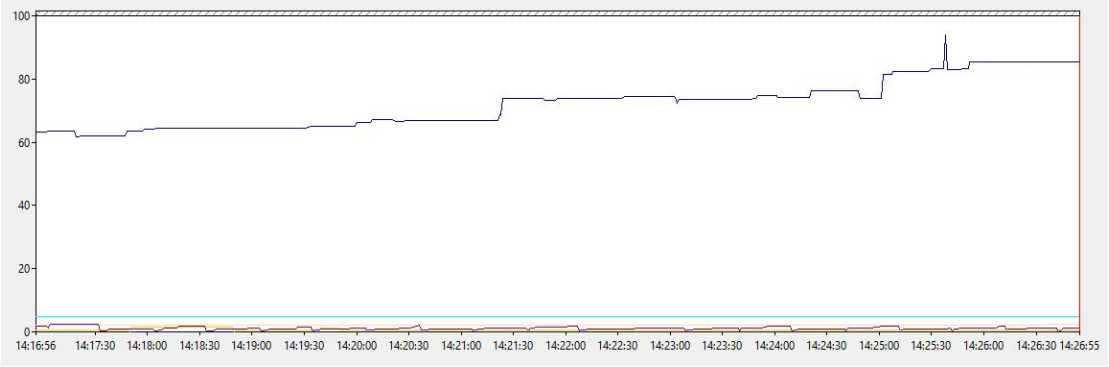
Gdzie - 1: składnik ochrony aktywny, 0: składnik ochrony nieaktywny (ustawienia wg pliku XML z pobranym instalatorem EXE)

```
<features>
<feature name="FileScan" action="1"/>
<feature name="UserControl" action="1"/>
<feature name="Antiphishing" action="1"/>
<feature name="Firewall" action="1"/>
<feature name="UpdateServer" action="0"/>
<feature name="BehavioralScan" action="1"/>
<feature name="TrafficScan" action="1"/>
<feature name="MailServers" action="0"/>
<feature name="DataLossPrevention" action="1"/>
<feature name="PowerUser" action="1"/>
</features>
...
<scanType strVar="ScanType">light</scanType>
```

Tryb jałowy:

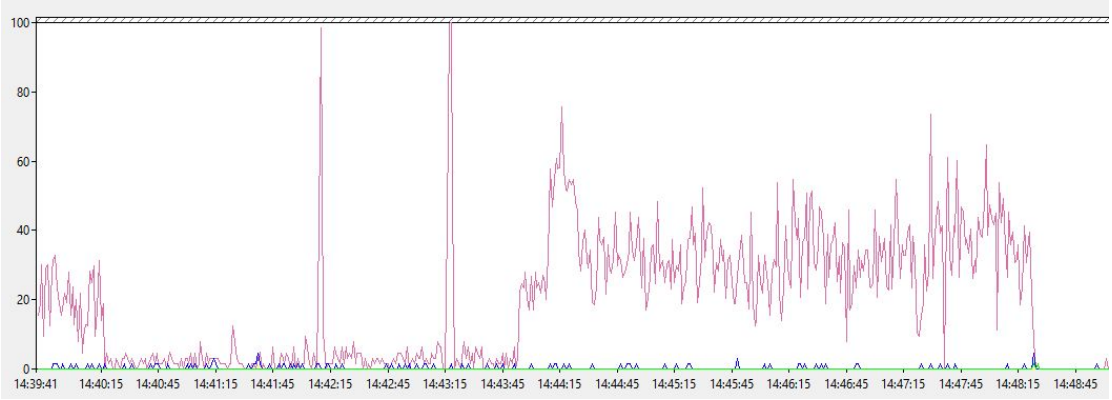


W spoczynku, zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 0,645%. Drugi rdzeń nie był obciążony.

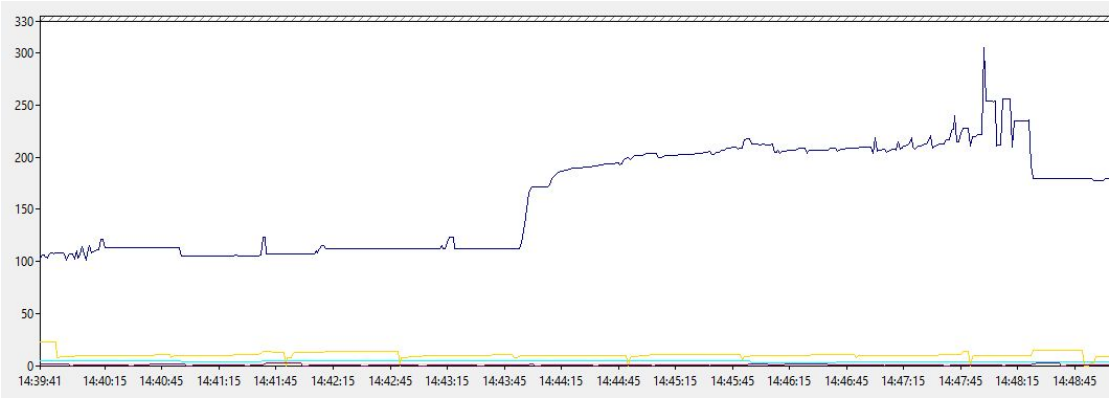


W spoczynku, procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~77MB pamięci RAM

Skanowanie pełne (wszystkich dysków):



Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 19,059%. Drugi rdzeń nie był obciążony. Maksymalna wartość skokowa osiągnęła ~104%, co oznacza, że jeden rdzeń w tej konkretnej sekundzie został obciążony w 100%, a drugi w ~4%.



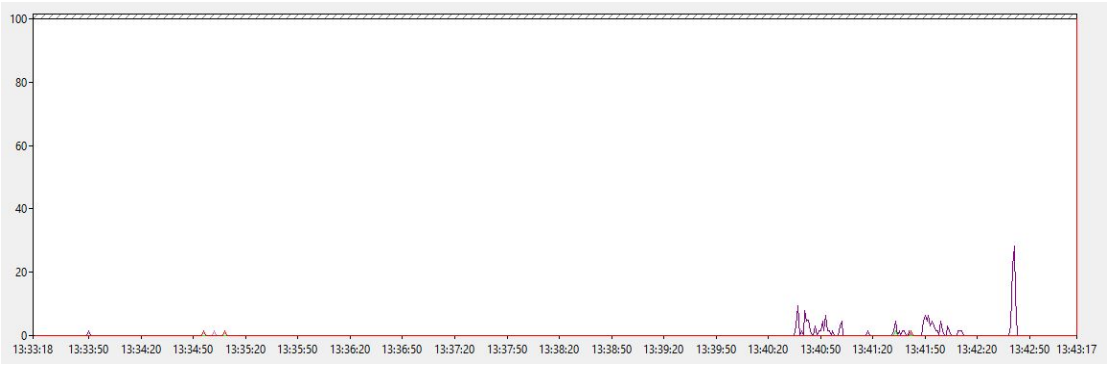
Podczas skanowania, średnio procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~176MB pamięci RAM.

Skanowanie centralne

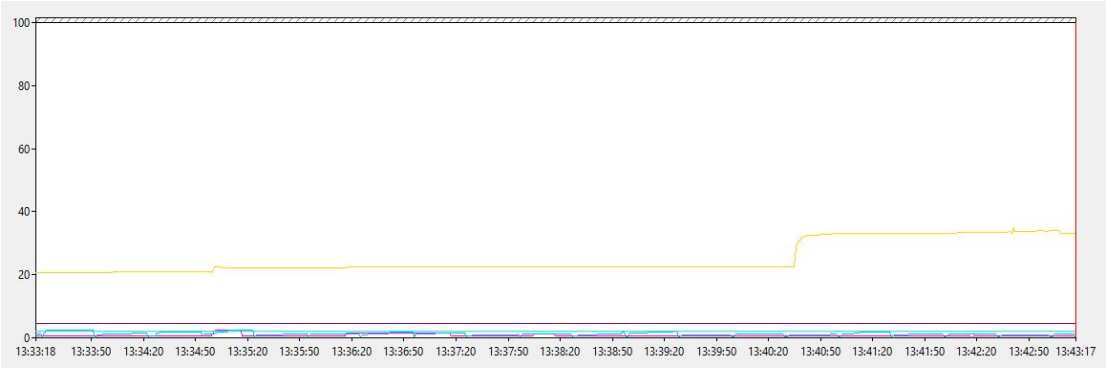
Gdzie - 1: składnik ochrony aktywny, 0: składnik ochrony nieaktywny (ustawienia wg pliku XML z pobranym instalatorem EXE)

```
<features>
       <feature name="FileScan" action="1"/>
       <feature name="UserControl" action="1"/>
       <feature name="Antiphishing" action="1"/>
       <feature name="Firewall" action="1"/>
       <feature name="UpdateServer" action="0"/>
       <feature name="BehavioralScan" action="1"/>
       <feature name="TrafficScan" action="1"/>
   <feature name="MailServers" action="0"/>
   <feature name="DataLossPrevention" action="1"/>
   <feature name="PowerUser" action="1"/>
</features>
...
<scanType strVar="ScanType">remote</scanType>
```

Tryb jałowy:

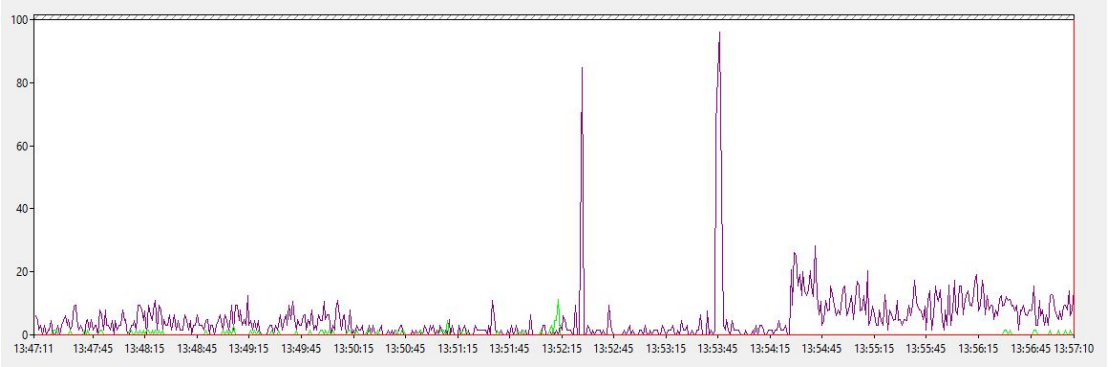


W spoczynku, zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 0,344%. Drugi rdzeń nie był obciążony.

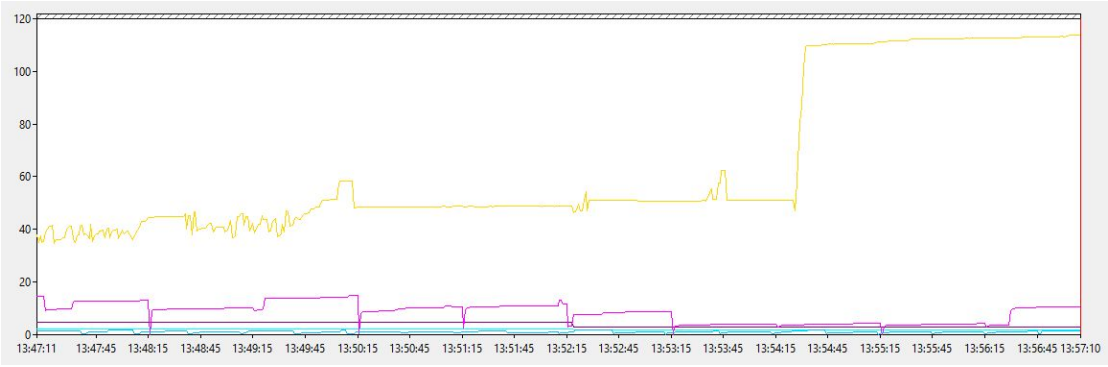


W spoczynku, procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~33MB pamięci RAM

Skanowanie pełne (wszystkich dysków):



Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 5,307%. Drugi rdzeń nie był obciążony.



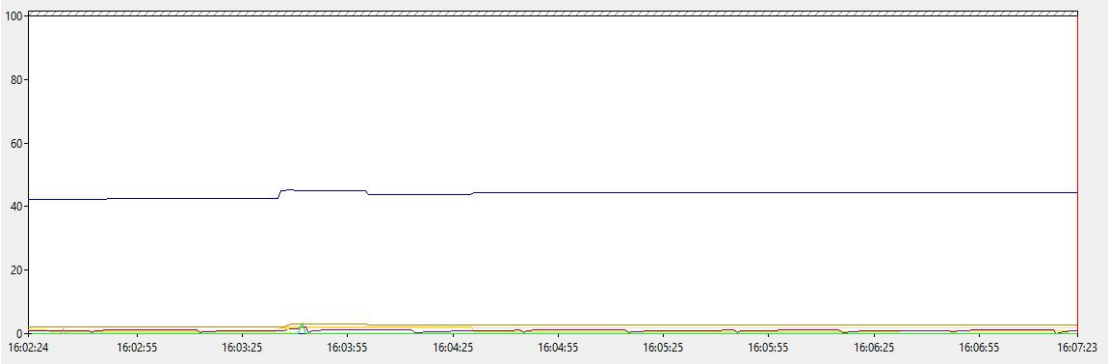
Podczas skanowania, średnio procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~76MB pamięci RAM.

Powtórzenie pomiarów

Dla lepszego porównania wydajności, skanowanie powtórzono dnia kolejnego. Wyniki zbierano przez 5 minut. Ponieważ testowy system wirtualny zawierał podstawowe oprogramowanie, a czas skanowania zakończyłby się przed czasem pomiarowych 10 minut, wyniki zbierano przez 5 minut.

Poniższe wykresy są zbiorcze, co oznacza, że zawierają pomiary zarówno dla RAM, jak i CPU.

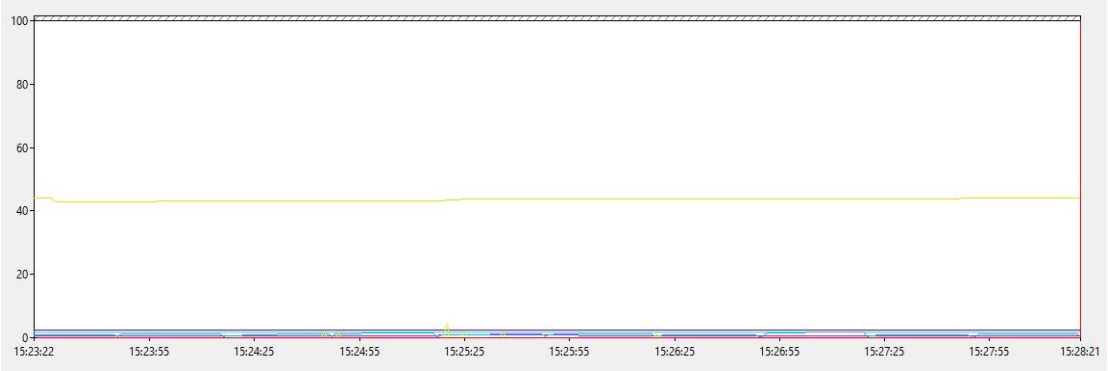
Ustawienia: skanowanie lokalne:



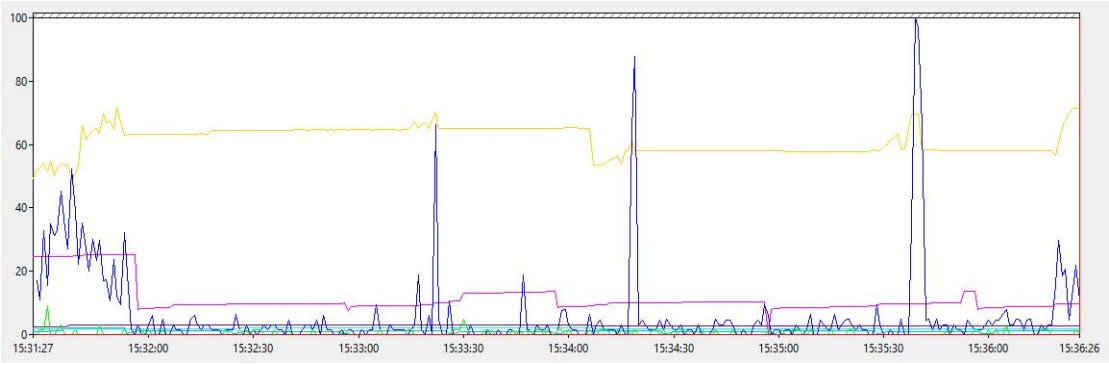
W spoczynku, zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wynosił 0,030%. Drugi rdzeń nie był obciążony. W spoczynku, procesy Bitdefender Endpoint Security Tools potrzebowały do działania ~48MB pamięci RAM.

Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 6,156%. Procesy potrzebowały do działania ~81MB pamięci RAM.

Skanowanie hybrydowe:

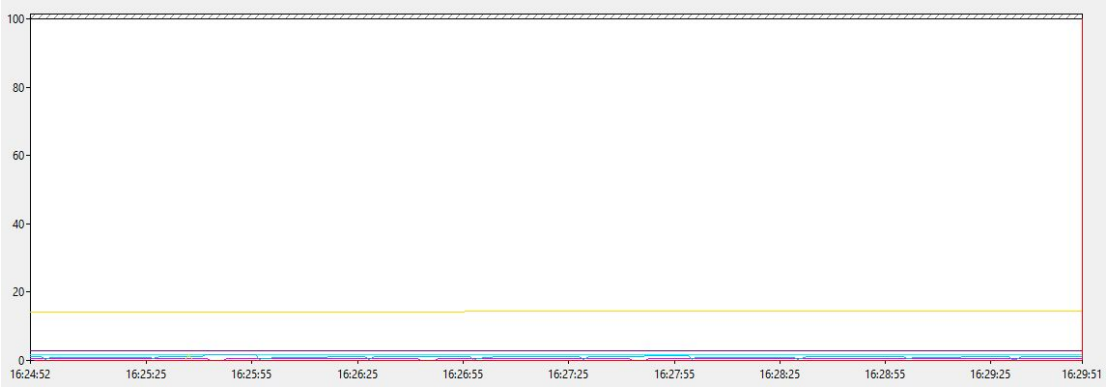


W spoczynku, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 0,042%. Procesy potrzebowały do działania ~47MB pamięci RAM.

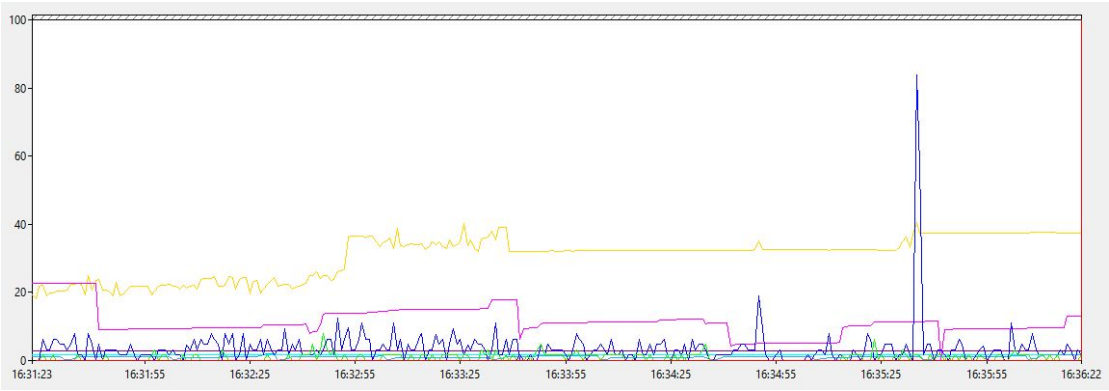


Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 6,835%. Procesy potrzebowały do działania ~75MB pamięci RAM.

Skanowanie centralne:



W spoczynku, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 0,005%. Procesy potrzebowały do działania ~19MB pamięci RAM.



Podczas skanowania, średnie zapotrzebowanie procesów Bitdefender Endpoint Security Tools na czas jednego rdzenia procesora wyrażony w [%] wyniosło 4,396%. Procesy potrzebowały do działania ~47MB pamięci RAM.

Podsumowanie

Pomiar pierwszego dnia:

Tryb jałowy			
	Lokalne	Hybrydowe	Centralne
CPU [%]	0,918	0,645	0,344
RAM [MB]	67	77	33

Skanowanie			
	Lokalne	Hybrydowe	Centralne
CPU [%]	18,121	19,059	5,307
RAM [MB]	164	176	76

Drugi pomiar dnia kolejnego:

Tryb jałowy			
	Lokalne	Hybrydowe	Centralne
CPU [%]	0,030	0,042	0,005
RAM [MB]	48	47	19

Skanowanie			
	Lokalne	Hybrydowe	Centralne
CPU [%]	6,156	6,835	4,396
RAM [MB]	81	75	47

Rozmiar po instalacji agenta		
Ustawienia lokalne	Ustawienia hybrydowe	Ustawienia centralne
~580MB	~378MB	~320MB

Różnice pomiędzy skanowaniem w pierwszym dniu a drugim są dla nas oczywiste, jednakże wymagają kilka słów wyjaśnienia.

Test został przeprowadzony na trzech identycznych kopiach systemu operacyjnego. W ten sposób nie jest pomijana kwestia buforowania dostępu do plików przez system plików, przez co kolejny program antywirusowy może działać szybciej niż pierwszy.

W większości przypadków, programy antywirusowe, które przeskanują pliki, nie sprawdzają ich ponownie, aż do ich modyfikacji (próby odczytu / zapisu). Specjalny algorytm może oceniać, czy plik został już przeskanowany, dzięki czemu program antywirusowy mógłby wypaść lepiej w teście. Z tego też powodu, uruchomienie skanowania on-access lub on-demand powoduje, że drugi test może zostać zakończony dużo szybciej.

Zdecydowaliśmy się przeprowadzić w ten sposób testy, aby udowodnić, że zalecenia wszystkich producentów antywirusów nie są bezpodstawne. Aby zmniejszyć zużycie zasobów potrzebnych do działania programu antywirusowemu, należy bezzwłocznie po jego zainstalowaniu uruchomić pełne skanowanie wszystkich dysków. Im bardziej w czasie decyzja ta jest odwlekana, tym gorzej dla pracownika, który jest zmuszony korzystać ze stacji roboczej o starej konfiguracji sprzętowej.

Opatentowana przez firmę Bitdefender technologia centralnego skanowania środowisk wirtualnych odwzorowała w naszym teście to, do czego została zaprojektowana. W skanowaniu tym nie biorą udziału lokalne sygnatury, ani żadne metody skanowania za pośrednictwem chmury, dlatego zapotrzebowanie agenta na pamięć operacyjną oraz procesor jest tak niewielkie.

Szczegóły na temat działania centralnego skanowania opisano w artykule “Bitdefender GravityZone Virtual Appliance dedykowany dla środowisk wirtualnych”

Bitdefender GravityZone

Kilka słów o AVLab

AVLab skupia w jednym miejscu miłośników oprogramowania antywirusowego oraz bezpieczeństwa w Internecie. Nasze działania obejmują testowanie programów i dzielenie się wynikami z naszych analiz ze wszystkimi użytkownikami. Nie jesteśmy kontrolowani i/lub powiązani w jakikolwiek sposób z żadnym producentem oprogramowania.

Testy AVLab są niezależne i odbywają się w warunkach zbliżonych do rzeczywistości. Nie należy kierować się naszymi wynikami jako ostateczną decyzją w wyborze programu antywirusowego. W celu dokonania wyboru, sugerujemy zapoznać się także z testami innych niezależnych laboratoriów, które korzystają z różnych metod i technik testowania oprogramowania antywirusowego. Ponadto, decyzje w wyborze zależą od osobistych preferencji, dostępności niezbędnych funkcji, skuteczności, wykrywalności, wpływu na wydajność systemu, wyglądu interfejsu, ceny, łatwości użytkowania, kompatybilności, języka, wsparcia technicznego i wielu innych cech.

Więcej informacji o produktach firmy Bitdefender:
https://avlab.pl/producent/bitdefender

Przyznane certyfikaty do pobrania w wysokiej rozdzielczości
https://avlab.pl/dla-prasy

Kontakt w sprawie testów
kontakt@avlab.pl