



VirusBuster
for NetWare Servers

SPIS TREŚCI

VIRUSBUSTER FOR NETWARE SERVERS	2
Minimalne wymagania systemowe	2
Instalacja	3
Instalacja automatyczna	3
Instalacja manualna	3
Struktura programu	4
Możliwości skanowania	4
Chronione obszary	5
Interfejs użytkownika	5
Szczegółowy opis programu	6
Engine options - Opcje silnika	6
Domain management – Zarządzanie domenami	9
Message redirection – Wysyłanie powiadomień	11
Global options – Ogólne opcje programu	15
Quarantine - Kwarantanna	16
Information - Informacje	16
Runtime options – Ustawienia uruchamiania	16
Registration - Rejestracja	16
UPDATE MANAGER – MENEDŻER AKTUALIZACJI	18
Settings - Ustawienia	18
Module versions – wersje modułów	19
Manual update – aktualizacja manualna	19
Information – Informacje	20
END USER AGREEMENT	21
CONTACT	22

VIRUSBUSTER FOR NETWARE SERVERS

W otoczeniu sieciowym zabezpieczanie serwerów jest niezbędne, ponieważ wszystkie dane, których używamy w codziennej pracy są przechowywane i przesyłane za ich pomocą. Dlatego też efektywne zabezpieczenie serwerów chroni nie tylko przechowywane informacje, ale zapewnia drugą linię ochrony dla klientów podłączonych do nich.

VirusBuster for NetWare Servers umożliwia rezydentną ochronę danych, systemów i dlatego codzienne działanie optymalizuje wzrastający ruch danych na serwerach. Prosty w obsłudze, wykorzystujący tradycyjny interfejs użytkownika NetWare, zawierający przejrzyste ustawienia i zapewnia stałą aktualizację. To powoduje, że zabezpieczenie serwerów firmy działa automatycznie i efektywnie.

Podstawowe cechy programu:

- Efektywna ochrona użytkownika przed wirusami w trakcie korzystania z serwerów.
- Niezależne obszary ochrony pozwalające chronić całe magazyny danych lub wydzielone części
- Inteligentna ochrona plików, rozszerzona ochrona zapisu chroniąca przed incydentami.
- Skanowanie manualne i wg harmonogramu.
- Automatyczne uaktualniania.
- Inteligentna kwarantanna zarażonych plików.
- Codzienna aktualizacja bazy wirusów.

Minimalne wymagania systemowe

Do uruchomienia programu niezbędne są następujące parametry systemu:

- Novell NetWare Server 5.1+SP8, 6+SP5, 6.5+SP8
- Intel Pentium (lub kompatybilny) z zegarem
- 1024 MB pamięci RAM (Novell NetWare 6.x: 2048 MB)
- 150 MB wolnego miejsca na dysku.

Instalacja

Produkt jest dystrybuowany w postaci samorozpakowującego się pliku (.exe) lub w postaci spakowanego pliku .zip. Użyj wersji samorozpakowującej lub skorzystaj z programu rozpakowującego pliki typu .zip.

Instalacja automatyczna

Program dystrybuowany jest w postaci następującego pliku:

`nwshield-<product version>-<engine version>-<language>.exe`

Przykładowo:

`nwshield-2.2.08-4.2.13-en.exe`

- Po pojawieniu się okna powitalnego wraz z licencją użytkownika, możesz wybrać docelowy folder instalacji, w którym program zostanie zainstalowany.
- Po wskazaniu docelowego folderu zostanie pokazana wersja modułów do zainstalowania, po to abyś mógł je wybrać i sprawdzić.
- Na następnym oknie możesz wybrać składniki programu, które chcesz zainstalować. Główny moduł jest niezbędnym elementem a Update Manager (Menedżer aktualizacji) jest opcjonalny.
- Po naciśnięciu przycisku **[Next>]**, będziesz mógł ustawić zadania, które zostaną automatycznie uruchomione w końcowej fazie instalacji.

Uwaga!

Jeśli któreś z zadań nie będzie mogło być uruchomione, należy uruchomić je ręcznie po zakończeniu instalacji, opierając się na sekcji *Instalacja manualna*.

Zadania, które możesz wskazać w tym miejscu są identyczne, jak te określone w manualnej instrukcji instalacji (porównaj z sekcją *Manualna instalacja*).

VirusBuster for NetWare Servers – VirusBuster for NetWare Servers

- *Start protection – Włącz ochronę:* Jeśli zostanie zaznaczone, ochrona antywirusowa będzie automatycznie uruchomiona po zakończeniu instalacji.

- *Modify autoexec.ncf – Zmodyfikuj autoexec.ncf:* Jeśli zostanie zaznaczone, będą wykonane niezbędne modyfikacje pliku `autoexec.ncf` (porównaj z sekcją *Instalacja manualna*).

- *Registration - Rejestruj:* Jeśli zostanie zaznaczone, będziesz mógł wprowadzić dane niezbędne do rejestracji programu podczas instalacji.

VirusBuster Update Manager – Menedżer aktualizacji VirusBuster

- *Start module module – Uruchom moduł:* Jeśli zostanie zaznaczone, moduł Menedżera aktualizacji będzie automatycznie uruchomiony po zakończeniu instalacji.

- Jeśli zaznaczyłeś powyżej opcję *Rejestruj*, teraz będziesz mógł wpisać poprawne dane rejestracyjne.
- Po ustawieniu wszystkich parametrów, program instalacyjny zostanie uruchomiony, a wskazane zadania zostaną zrealizowane.

Instalacja manualna

Program dystrybuowany jest w postaci następującego pliku:

`nwshield-<product version>-<engine version>-<language>.zip`

Przykładowo:

`nwshield-2.2.08-4.2.13-en.zip`

Program może być uruchomiony na serwerach Novell NetWare i musi być umieszczony na woluminie

SYS: serwera w podkatalogu tak, aby mógł być uruchamiany z konsoli. Instalacja powinna być przeprowadzona z uprawnieniami administracyjnymi.

Kroki, jakie należy wykonać przy pierwszej instalacji:

- Zaloguj się na konto administratora domeny. Utwórz podkatalog o nazwie **vbuster** w katalogu **SYS:\SYSTEM**. Konfiguracja pliku, pliku rejestru (log), **QUAR** (kwarantanna) i katalog tymczasowy **TEMP** zostaną tutaj utworzone automatycznie. Dodaj nowy katalog do ścieżki przeszukiwania używając polecenia:
`search add sys:system/vbuster`
- Przekopiuj pliki programu (**VBSHLD4.NLM**, **VBENGINE.NLM**, **VBUSTER.INI** i oraz bazę antywirusową (Biblioteki **DATABASE** i jej zawartość)). Skopiuj również pliki niezbędne do automatycznej aktualizacji: **VBUPDATE.NLM** i **VBUPDASC.NLM**.
- Dodaj nową linię `search add 1 sys:system/vbuster` do pliku **SYS:SYSTEM/AUTOEXEC.NCF**. Jeżeli chcesz, aby ochrona była uruchamiana automatycznie z serwerem powinieneś wprowadzić także następujący wiersz: `load vbshld4.nlm`. Plik **SYS:SYSTEM/AUTOEXEC.NCF** może być modyfikowany za pomocą dowolnego edytora tekstu ze stacji roboczej albo poprzez program **INSTALL.NLM** z serwera (właściwości pliku NCF / Edytuj plik **AUTOEXEC.NCF**).
- Utwórz nowego użytkownika z prawami administratora poprzez program administracyjny Novell NetWare's (NetWare Administrator lub ConsoleOne) przeznaczonego wyłącznie do uruchamiania ochrony antywirusowej. Rekomendowana nazwa użytkownika to *vbuster*. Użytkownik ten powinien zostać dodany do specjalnej grupy użytkowników programu.
- Uruchom program na serwerze używając polecenia **vbshld4** i przeprowadź konfigurację programu.

Jeżeli wszystko jest w porządku, moduły zostaną załadowane i dwie nowe pozycje zostaną wyświetlone na ekranie konsoli (VBSShield Screen i konsoli VBSShield).

Struktura programu

VirusBuster for NetWare Servers jest ładowalnym modułem NetWare (NLM), który powinien być uruchomiony na serwerze. Po tym jak zostanie zainstalowany, sprawdza każdą operację wykonaną przez serwer i skanuje każdy plik przed wykonaniem operacji na nim. Jeżeli znajdzie wirusa w skanowanym pliku, rozpoczyna działanie określone w konfiguracji programu. Może odmówić wykonania polecenia, umieścić zainfekowany plik w kwarantannie, wyleczyć go i wysłać powiadomienie do odpowiednich użytkowników lub administratora domeny. Umieszcza wszystkie niezbędne informacje dot. operacji w pliku rejestru (log).

Istnieje możliwość zdefiniowania praw dostępu do pliku przekraczających standardowe możliwości Novell NetWare. Zapisywanie w katalogach sieciowych może być także prosto ograniczone chroniąc przed zakażeniem wirusem.

Możliwości skanowania

VirusBuster for NetWare Servers skanuje pliki na dwa sposoby. Z jednej strony monitoruje wszystkie operacje wykonywane na plikach wykonywane na serwerze, innymi słowy: sprawdza każde przychodzące zapytania i pozwala na dostęp tylko do zdrowych plików. Z drugiej strony skanowanie wirusów może się odbywać na żądanie wg harmonogramu dla wskazanych obszarów ochrony, które mogą być ustalone albo mogą być manualnie uruchamiane z konsoli.

- On access scan – Skanowanie w trybie dostępu do pliku
W przypadku skanowania w trybie dostępu do pliku program automatycznie sprawdza pliki, które chcemy otworzyć. Rodzaje plików, które powinny zostać zeskanowane mogą być ustawione inaczej dla każdej domeny. Istnieją dwie listy do tego celu; pierwsza zawiera wzorce plików do zeskanowania, a druga zawiera wzorce wyjątków.
- Periodical scan – Skanowanie wg harmonogramu
W przypadku skanowania wg harmonogramu wszystkie pliki w domenie będą zeskanowane. Skanowanie wg harmonogramu może być zainicjowane manualnie lub automatycznie w czasie określonym dla każdej domeny indywidualnie.
- Write protection of files – Ochrona zapisu plików
Umożliwia ochronę plików w trakcie zapisu poprzez wsparcie systemu ochrony dostępu do plików sieciowych Novell NetWare. Ochrona zapisu jest niezależna od praw użytkowników. Innymi słowy dotyczy wszystkich użytkowników. Dla każdej domeny system ochrony plików może być włączony bądź wyłączony, jak również dla każdej z nich można określić wzorce skanowanych plików i wyjątki.

Chronione obszary

Podobnie do systemu ochrony kontekstowej Novell NetWare, opcje skanowania i ochrony dla VirusBuster for NetWare Servers mogą być ustawione niezależnie dla każdej domeny. Jedna struktura podkatalogów serwera należy do chronionego obszaru. Jeśli taka struktura nie zawiera dalszych chronionych obszarów, to ustawienia będą dotyczyły wszystkich podkatalogów i plików w tym katalogu. Jeśli struktura podkatalogów zawiera dalsze obszary chronione, to nadrzędne ustawienia nie będą zastosowane do wydzielonych obszarów. Podsumowując, plik może należeć tylko do jednego obszaru ochrony.

Interfejs użytkownika

Funkcje i ustawienia programu są dostępne poprzez standardowe menu systemu Novell NetWare. Po uruchomieniu programu funkcje i parametry są dostępne w menu.

Używanie menu

- Klawisze kursora - przemieszczanie się pomiędzy pozycjami menu
- **Klawisz Enter** - wybór pozycji menu
- **Klawisz ESC** - wyjście z podmenu lub z programu
- **Klawisz F1** - wyświetla okno pomocy programu

W programie podstawową jednostką do konfiguracji jest lista. Zawartość listy może być modyfikowana, usuwana i dodawana, a także konfigurowana bardziej szczegółowo przy użyciu następujących klawiszy:

Używanie list

- Klawisze kursora, **PgDn**, **PgUp** - przemieszczanie się pomiędzy pozycjami listy
- **Klawisz Enter** - wybór jednego lub więcej pozycji listy
- **Klawisz F5** - zaznaczanie bądź odznaczanie pozycji
- **Klawisz Delete** - usuwanie pozycji
- **Klawisz Insert** - dodawanie pozycji
- **Klawisz F3** - zmiana nazwy pozycji

Podczas wpisywania danych pola wymagane są oznaczone * (gwiazdką).

Wprowadzanie dat

- Klawisze kursorów za pomocą, których możesz poruszać się w obrębie arkusza.
- Określenie okresu jest możliwe poprzez klawisz **F5**.
- Naciskając klawisz Insert lub gwiazdkę (*) można wskazać datę lub wpisać okres
- Naciskając klawisz **Delete** lub **Space** aktualna data zostanie odznaczona
- Naciskając klawisz **Enter** można odwrócić stan zaznaczenia daty lub okresu

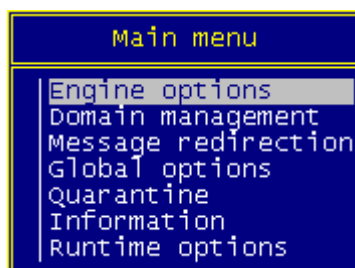
Szczegółowy opis programu

Program uruchamia się za pomocą pliku **VBSHLD4.NLM**. Program tworzy dwa okna:

- Okno VBShield – Monitorowane są tutaj zachowanie i zdarzenia programu
- Konsola VBShield – Program może być tutaj konfigurowany, dodawane mogą być tutaj indywidualne opcje i z tego miejsca można manualnie uruchamiać skanowanie wg harmonogramu.

Uwaga!

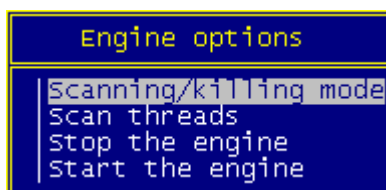
Jeżeli wyjdiesz z programu lub zamkniesz okno, ochrona zostanie zakończona. Po wyjściu, skanowanie okresowe nie zostanie wykonane.



Menu główne

Więcej informacji na temat programu uzyskasz korzystając bezpośrednio z pozycji menu.

Engine options - Opcje silnika



Opcje silnika

Scanning/killing mode - Tryb wyszukiwania i usuwania

```
Scanning/killing mode
Scan packed/MIME files: Enabled
Temporary directory: SYS:\SYSTEM\vbuster_ ...
Scan: strict
Virus killing: Disabled
Non-killable viruses: Keep file
In case of protection error: Access enabled
General heuristics: Normal
Suspicious programs: Keep file
```

Opcje trybu wyszukiwania i usuwania

Scan packed/MIME files - Skanowanie plików archiwalnych/Pliki MIME

Jeżeli jest aktywne, program będzie poszukiwał wirusów w skompresowanych plikach i w plikach MIME.

Temporary folder - Folder tymczasowy

Podczas skanowania program tymczasowo umieszcza zawartość plików skompresowanych i MIME w określonym w tym miejscu katalogu.

Scan - Skanowanie

Metoda skanowania może korzystać z następujących opcji:

- Strict - Optymalna: zoptymalizowana metoda skanowania wyszukująca wirusy w tych częściach pliku, gdzie zwykle wirusy się zagnieżdżają.
- Fast - Szybka: metoda skanowania poszukuje wirusów tylko w tych częściach pliku gdzie zwykle się one znajdują. Metoda ta jest rekomendowana w większości przypadków.
- Full - Pełna: skanuje cały plik, nawet miejsca gdzie w normalnych warunkach wirusy nie występują, tym samym wzrasta szansa na fałszywe alarmy. Metoda ta jest czasochłonna.

Virus killing – Niszczanie wirusów

W przypadku gdy jest to możliwe program ma usuwać wirusy z zarażonego pliku.

Non-killable viruses – Nieusuwalne wirusy

Niektóre wirusy nie mogą zostać usunięte nawet, jeżeli zostaną wykryte. Ten parametr umożliwia ustawienie opcji, co zrobić z takimi plikami.

- Rename file - Zmiana nazwy pliku: zmień nazwę zarażonego pliku.
- File to quarantine – Przenieś plik do kwarantanny: przenieś zarażony plik do katalogu kwarantanny.
- Keep file - Pozostaw plik bez zmian: nie wykonuj żadnych operacji na zarażonym pliku.
- Delete file - Usuń plik: usuń zarażony plik.

In case of protection error – W przypadku błędu ochrony

W przypadku błędu ochrony można ustawić czy dostęp do pliku ma zostać zablokowany czy też nie.

General heuristics - Heurystyka (wyszukiwanie nieznanych wirusów)

Skanowanie heurystyczne może być włączone lub wyłączone a także można ustalać poziom takiej analizy. Podczas analizy heurystycznej program próbuje wykryć kod charakterystyczny dla wirusów w plikach, nieznanych dotąd za wirusy. Użytkownik będzie powiadomiony, jeżeli taki podejrzany plik

zostanie znalezione.

Dostępne są następujące poziomy analizy heurystycznej:

- *Disabled - Wyłączony*
Nie ma analizy heurystycznej.
- *Normal - Standardowy*
Ustawienie to powoduje niski poziom fałszywych wskazań przy niewysokim stopniu wyszukiwania nieznanymi wirusów.
- *Strong - Wysoki*
Szansa wykrycia nienanego wirusa jest wyższa, ale istnieje także wyższe prawdopodobieństwo błędnych wskazań.

Suspicious programs – Podejrzane programy

Poniższe ustawienia dotyczą plików uznanych za podejrzane w trakcie analizy heurystycznej:

- Rename file - Zmiana nazwy pliku: zmień nazwę zarażonego pliku.
- File to quarantine – Przenieś plik do kwarantanny: przenieś zarażony plik do katalogu kwarantanny.
- Keep file - Pozostaw plik bez zmian: nie wykonuj żadnych operacji na zarażonym pliku.
- Delete file - Usuń plik: usuń zarażony plik.

Scan threads - Wątki skanowania

Liczba jednoczesnych wątków skanowania.

```
Scan threads
Total number of scanner threads: 16
(Max.: 16, min.: 2!)
Reserved for on-access scan: 13
(Max.: total-1, min.: 1!)
```

Opcje liczby wątków skanowania

Uwaga! Wartość musi być zawarta pomiędzy 2 a 16. Nowa wartość zostanie zastosowana w momencie ponownego uruchomienia silnika skanowania!

Program wykorzystuje domyślnie cztery wątki. Dwa z nich są zarezerwowane do obsługi przychodzących zapytań podczas skanowania on-access (w trybie skanowania podczas dostępu do pliku). Zwiększenie liczby wątków może wpływać na obniżenie wydajności systemu jednakże pozwala zeskanować więcej plików w tym samym czasie.

Stop the engine - Zatrzymanie silnika

Rzadko się zdarza, że chcemy zatrzymać tylko silnik skanowania niezależnie od reszty programu, ale może być to użyteczne podczas uaktualniania programu. Jednakże należy pamiętać, że silnik może być uaktualniany podczas pracy.

Uwaga!

Pomimo zatrzymania silnika ochrona pozostaje nadal aktywna, ale skanowanie nie odbywa się. Następstwem tego może być brak dostępu do ważnych plików.

Start the engine – Uruchomienie silnika

Uruchomienie silnika i załadowanie aktualnej bazy deskryptorów (VDB file) z ustawieniem wersji bazy.

Uwaga! Upewnij się, że pliki VBENGINE.NLM i bazy wirusów znajdują się na ścieżce wyszukiwania. Plik VBENGINE.NLM zostanie załadowany tylko wtedy, gdy wersja bazy wirusów i VBENGINE.NLM będzie właściwa.

Domain management – Zarządzanie domenami

Wszystkie chronione domeny są wymienione w oknie "Domain entries list". W obrębie powyższej listy mogą być tworzone, usuwane lub może być zmieniana ich nazwa..

Ochrona domeny głównej / (root) nie może być usunięta i nie może być zmieniona jej nazwa. W momencie zmiany nazwy domeny (Klawisz **F3**) wszystkie związane z nią wpisy także zostaną zmienione. Jeżeli domena zostanie usunięta (Klawisz **Delete**) pozycje z nią związane także zostaną usunięte i jeśli jakikolwiek serwis pocztowy zostanie zatrzymany program o tym ostrzeże użytkownika. Jeżeli skanowanie wg harmonogramu jest wykonywane na domenę, która została usunięta lub została zmieniona jej nazwa skanownie zostanie natychmiast zatrzymane. Jeżeli zostanie utworzona nowa domena będzie ona posiadała właściwości wskazanej domeny, która zostanie wybrana poprzez wciśnięcie klawisza **Insert**.

Uwaga! Pamiętaj, że domena nie będzie chroniona podczas zmiany konfiguracji, dlatego nie pozostawiaj okna konfiguracji otwartego!

Poniższe ustawienia mogą być zmienione wewnątrz sekcji dotyczącej ochrony domeny:

```
SYSTEM
Domain path: SYS:SYSTEM
On-access scan: Enabled
Virus found action: Access denied
Periodic scan: (time table)
Files to be scanned: (list)
Exceptions: (list)
Write protection of files: Enabled
Write protected files: (list)
Exceptions: (list)
```

Ustawienia domeny

Domain path – Ścieżka domeny

Wszystkie chronione domeny posiadają podkatalogi. Tutaj może być ustawiony podkatalog. Pełna ścieżka może być ustawiona w oknie **volume name:path**. Jeżeli określasz ścieżkę, katalog może być podzielony znakiem "/" lub "\".

On-access scan – Skanowanie w trybie dostępu do pliku

Skanowanie plików przechowywanych na serwerze w trybie dostępu do pliku (on-access) może być włączone bądź wyłączone. Program skanuje pliki w trybie bezpośredniego dostępu, jeżeli opcja ta jest włączona.

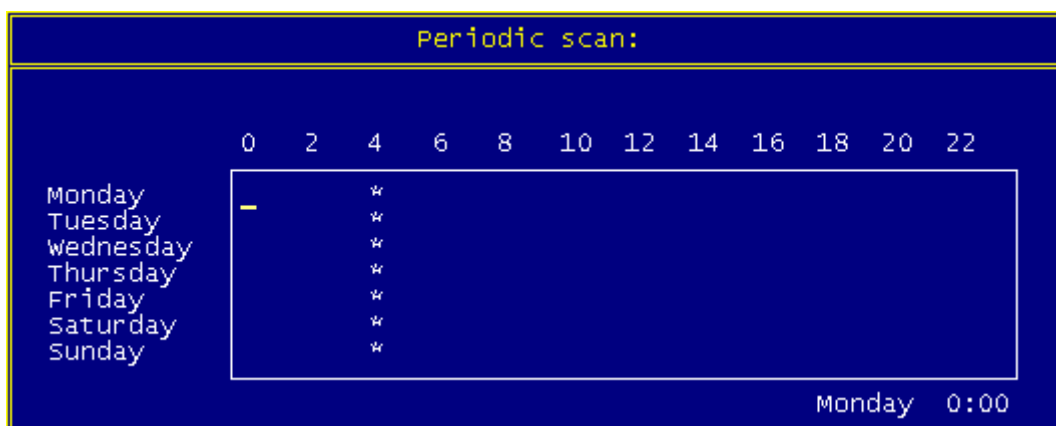
Virus found action – Akcja podejmowana przy znalezieniu wirusa

Jeżeli skanowanie plików w trybie bezpośredniego dostępu jest włączone, za pomocą poniższych ustawień możesz zdecydować, co zrobić w przypadku znalezienia wirusa:

- File to quarantine – Kwarantanna pliku: zarażony plik zostanie przeniesiony do katalogu określonego w ustawieniach ogólnych programu (Global options/Virus collector).
- Access denied – Zablokuj dostęp: brak dostępu do zarażonego pliku.
- No action – Nic nie rób: nie wykonuj żadnych operacji na zarażonym pliku.
- Delete file – Usuń plik: usuń zarażony plik.

Periodic scan – Skanowanie wg harmonogramu

Skanowanie wg harmonogramu może być ustawione w 30-to minutowych odstępach czasowych. Dlatego program może skanować w odstępach tygodniowych, dziennych i skanować wybrane katalogi domen o określonej porze. Jeśli program wykryje, że ma zadanie skanowania wykona je natychmiast.



Skanowanie wg harmonogramu

Files to be scanned – Pliki do skanowania

Wzorzec plików, który powinien zostać zekanowany może być wybrany tutaj (np. *.com, *.exe, *.doc).

Exception - wyjątki

Wzorzec plików, który nie powinien zostać zekanowany może być wybrany tutaj (np. command.com).

Write protection of files - Ochrona plików w trakcie zapisu

Ochrona plików w trakcie zapisu może być włączona lub wyłączona w tym miejscu. Ochrona ta nie dotyczy specjalnych użytkowników.

Write protected files – Pliki chronione podczas zapisu

W tym miejscu może zostać wybrany wzorzec (maska) chronionych podczas zapisu plików.

Exceptions - wyjątki

W tym miejscu może zostać wybrany wzorzec (maska) chronionych plików, które nie powinny (nie muszą) być chronione podczas zapisu.

Uwaga!

W trakcie uruchomienia programu zostanie utworzona domyślna konfiguracja, jeśli plik `VBUSTER.CFG` nie zostanie znaleziony w katalogu programu VirusBuster for NetWare Servers. W takim przypadku wszystkie pliki wykonywalne będą poddane skanowaniu. Skanowanie plików wykonywalnych w każdej domenie wg harmonogramu zostaje ustawione na godzinę 4 rano każdego dnia. Ochrona zapisu dotyczy tylko plików znajdujących się w katalogach `SYS:LOGIN`, `SYS:PUBLIC` i `SYS:SYSTEM`.

Message redirection – Wysyłanie powiadomień

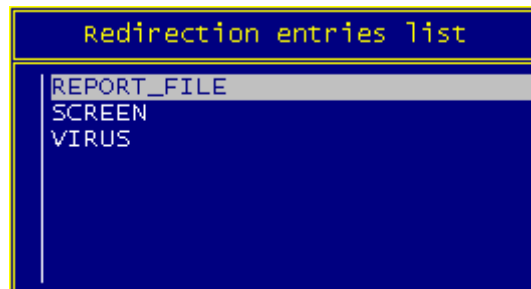
W tym menu program pokazuje nazwę powiadomienia. Pozycje powiadomień mogą być tworzone, kasowane lub może być zmieniana ich nazwa. Szczegółowe opcje powiadomienia są dostępne po jego wskazaniu.

Uwaga!

Powiadomienie jest nieaktywne podczas zmiany konfiguracji!

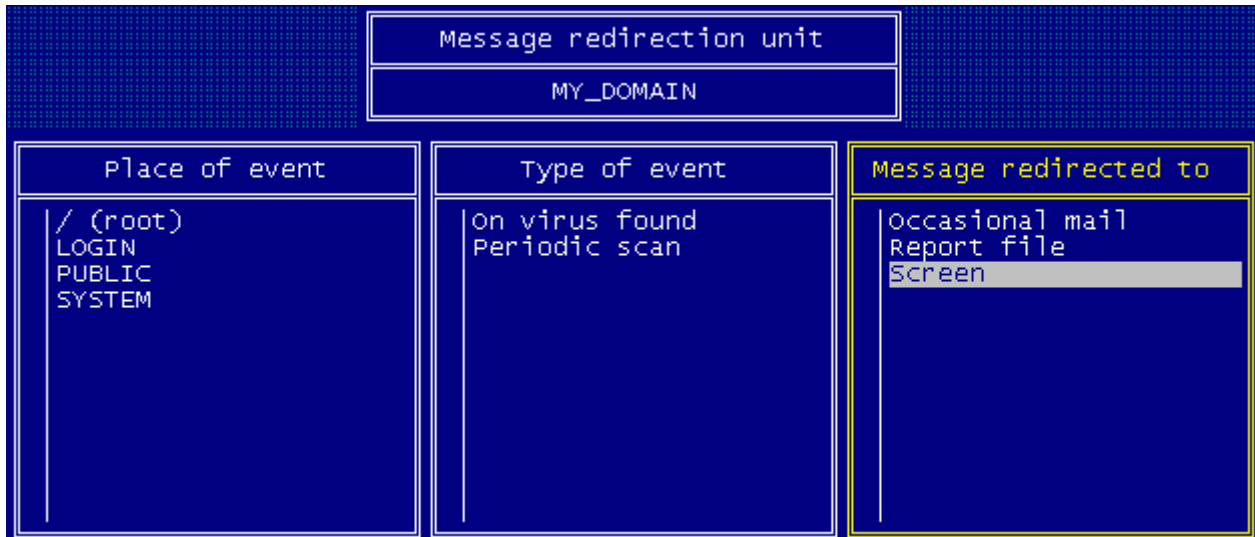
Podczas konfigurowania powiadomienia możesz wskazać, gdzie wiadomość powinna zostać przesłana w konsekwencji wystąpienia pewnych zdarzeń. Trzy typy powiadomienia są domyślnie włączone:

- Report file – Plik raportu: Plik rejestru (log), w którym przechowywane są informacje o wszystkich zdarzeniach systemu.
- Screen – Ekran: Okno komunikatów programu.
- Virus – Wirus: Powiadomienie, która zawiera zdefiniowane adresów i jest aktywowane w momencie znalezienia wirusa.



Domyślne powiadomienia

Podczas konfigurowania powiadomień, musisz wprowadzić następujące dane: gdzie powstało zdarzenie, jaki jest typ zdarzenia oraz to, gdzie powinno zostać wysłane powiadomienie:



Panel informacji o powiadomieniu

Place of event – Miejsce zdarzenia

Miejsce zdarzenia można określić za pomocą następujących parametrów:

General - Ogólnie

Określa miejsce zdarzenia, które nie może być powiązane z żadnym ze zdefiniowanych obszarów chronionych. W momencie określenia miejsca zdarzenia jako ogólne (general), oznacza to, że miało ono miejsce wewnątrz VirusBuster for NetWare Servers, co powoduje, że wiadomość nie może być przekierowana do obszaru chronionego.

Domain name – Nazwa domeny

Jeśli nazwa domeny może być znaleziona, pozycja będzie dotyczyła wiadomości utworzonych w podanym obszarze ochrony. Podczas tworzenia nowej pozycji, będzie ona dziedziczyła pełne cechy jednostki, która była zaznaczona za pomocą klawisza **Insert**. Te ustawienia można modyfikować.

Type of event – Typ zdarzenia

Jednostka kontroli wiadomości rozróżnia cztery podstawowe grupy zdarzeń:

File protection – Ochrona plików

Opisuje zdarzenia wywołane przez program VirusBuster for NetWare Servers. W momencie włączenia, program będzie wysyłał komunikaty wywołane podczas próby nielegalnego zapisu w jakiegokolwiek domenie zawartej na liście *Miejsce zdarzenia*.

Information - Informacja

Dotyczy zdarzeń wywołanych przez program VirusBuster for NetWare Servers ale nie powiązanych z jakimkolwiek chronionym obszarem. Program będzie wysyłał następujące typy komunikatów:

- Occasional mail has been sent – Wysłano jednostkowe powiadomienie: Program generuje komunikat potwierdzający, w momencie wysłania jednostkowego powiadomienia. Program przyłącza także oryginalną wiadomość.
- Component - Komponent: Wiadomości utworzone za pomocą zewnętrznych komponentów także będą zarejestrowane.
- Engine events – Silniki powiadomień: Program generuje wiadomość przy każdym zdarzeniu, które jest powiązane z silnikiem.

- File changed – Nastąpiła zmiana pliku: Jeśli został znaleziony wirus i zainfekowany plik został przeniesiony do wskazanego folderu lub zmieniono jego nazwę, program wysyła powiadomienie. Powiadomienie zawiera także opis błędu.
- Error message from engine – Błąd z silnika: Program generuje powiadomienie przy wystąpieniu jakiegokolwiek błędu powiązanego z silnikiem.
- Configuration has changed – Konfiguracja została zmieniona: Powiadomienie zostanie wygenerowane w momencie zmiany konfiguracji.
- VirusBuster for NetWare Servers has started – Program VirusBuster for NetWare Servers został uruchomiony: Program wygeneruje powiadomienie w momencie uruchomienia programu VirusBuster for NetWare Servers.
- VirusBuster for NetWare Servers has stopped – Program VirusBuster for NetWare Servers został zatrzymany: Program wygeneruje powiadomienie w momencie zatrzymania programu VirusBuster for NetWare Servers.
- Periodic mail has been sent – Wysłano okresowe powiadomienie: Program wygeneruje komunikat potwierdzający w momencie wysłania listu. Treść oryginalnego listu zostanie przytoczona.

Periodic scan – Skanowanie wg harmonogramu

Opisuje zdarzenia wywołane przez VirusBuster for NetWare Servers podczas skanowania systemu wg harmonogramu. Program wyśle komunikat opisujący status skanowania wg harmonogramu w podanych poniżej obszarach chronionych:

- File to be scanned – Plik do sprawdzenia: Program otrzymał nowy plik podczas skanowania wg harmonogramu. Komunikat zawiera nazwę obszaru skanowania i nazwę pliku.
- Scan sub-directory – Skanuj podkatalog: Program otrzymał nowy podkatalog do sprawdzenia wg harmonogramu. Komunikat zawiera nazwę chronionego obszaru i nazwę katalogu.
- Scan started – Skanowanie uruchomione: Skanowanie wg harmonogramu zostało uruchomione we wskazanym obszarze ochrony. Komunikat zawiera nazwę chronionego obszaru.
- Scan stopped – Skanowanie zatrzymane: Skanowanie wg harmonogramu zostało zakończone we wskazanym obszarze ochrony. Komunikat zawiera nazwę chronionego obszaru.
- Scan aborted – Skanowanie przerwane: Skanowanie wg harmonogramu zostało przerwane w jednym ze wskazanych obszarów ochrony. Komunikat zawiera nazwę chronionego obszaru.

On virus found – Zdarzenia przy znalezieniu wirusa

Opisuje zdarzenie wywołane przez system skanowania VirusBuster for NetWare Servers. Komunikat będzie wysłany, gdy wirus zostanie znaleziony, niezależnie od tego, czy nastąpiło to w wyniku skanowania on-access (w bezpośrednim dostępie) czy skanowania wg harmonogramu. W zależności, od rezultatów skanowania można wysłać następujący komunikat:

- Suspicious - Podejrzany: Program znalazł podejrzany kod, wskazujący, że plik jest zarażony.
- Immuniser - Wyleczony: Program znalazł plik, który został wyleczony przez skaner antywirusowy.
- Internet worm (I-Worm) – Robak internetowy (I-Worm): Program znalazł robaka internetowego rozprzestrzeniającego się poprzez e-mail.
- Mutant: Program odnalazł kod bardzo podobny do znanego wirusa.
- Sequence – Wzorzec wirusa: Program odnalazł w pliku wzorzec znanego wirusa.
- Non-killable - Niezniszczalny: Program znalazł zainfekowany plik, który nie może zostać wyleczony przez skaner antywirusowy.
- Packed - Spakowany: Program odnalazł skompresowany plik zawierający wirusa.
- Trojan program - Trojan: Program odnalazł plik zawierający trojana.
- Virus - Wirus: Program odnalazł wirusa.

Messages' recipients – Odbiorcy wiadomości

Wiadomości mogą być przekierowane do następujących miejsc docelowych:

Occasional mail – Incydentalne listy

Wysyła jednostkowy list do odbiorców określonych w ustawieniach ogólnych.

ErrorLog – Rejestr błędów (log)

Zapisuje informacje w rejestrze błędów Novell NetWare (`SYS:SYSTEM/SYS$LOG.ERR`).

User - Użytkownik

Jeśli zdarzenie, które wystąpiło, jest w jakikolwiek sposób powiązane z użytkownikiem, to program wyśle powiadomienie typu broadcast do tego użytkownika.

Screen - Ekran

Komunikat będzie wyświetlony na ekranie VBSshield na serwerze.

Console - Konsola

Komunikat będzie wyświetlony na konsoli systemowej serwera.

Operator

Komunikat będzie wysłany do wszystkich aktualnie zalogowanych operatorów. Lista operatorów musi zostać wypełniona zanim zostanie aktywowany mechanizm powiadomień.

Periodic mail – Wiadomość wg harmonogramu

Wysyła wiadomość wg podanych w opcjach ogólnych warunków.

Report file – Plik raportu

Zapisuje komunikat w pliku rejestru, który może być dowolnie określony, domyślnie jest to plik `vbuster.log`.

Type of message – Typ wiadomości

Można określić język powiadomienia i stopień szczegółowości. Poziom szczegółów może przyjmować następujące wartości:

Short - Krótka

Komunikat zawiera tylko jedną linię. Komunikaty typu broadcast muszą być krótkie.

Normal - Standardowa

Wiadomość zawiera wszystkie informacje o zdarzeniu z wyjątkiem:

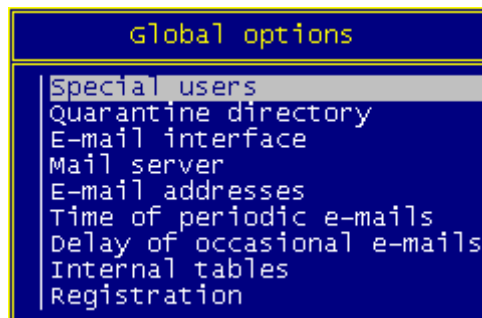
- Jeśli zdarzenie powiązane jest z plikiem, to jego ścieżka jest przedstawiona w uproszczonym formacie.
- Data zdarzenia nie jest pokazana.
- Nie zawiera fizycznego adresu źródła zdarzenia.

Detailed - Szczegółowa

Wiadomość zawiera wszystkie dostępne informacje o zdarzeniu.

Global options – Ogólne opcje programu

Ustawienia ogólnych opcji programu znajdują się w menu “Global options”.



Ogólne opcje programu

Special users – Użytkownicy specjalni

Tutaj może zostać określona lista użytkowników, którzy mogą odczytywać bądź zapisywać chronione pliki. Użytkownicy ci mogą uruchamiać proces naprawy plików w trakcie, gdy serwer (VirusBuster for NetWare Servers) jest uruchomiony. W takim przypadku użytkownicy ci nie muszą się wylogowywać z sieci.

Quarantine directory – Katalog kwarantanny

W momencie, kiedy użytkownik tego sobie życzy zarażony plik może być przeniesiony do tego katalogu.

E-mail interface – Stosowany interfejs e-mail

Za pomocą tej opcji można ustawić czy będą wysyłane wiadomości poprzez e-mail. Dostępne opcje:

- None: Program nie będzie wysyłał wiadomości
- Socket: Program będzie wysyłał wiadomości.

Mail server – Serwer pocztowy

Tu możesz wpisać nazwę domeny oraz adres IP serwera SMTP używanego do przesyłania wiadomości.

E-mail addresses – Adresy odbiorców

Tu wpisujesz listę osób, którzy będą otrzymywać powiadomienia pocztowe.

Time of periodic e-mails – Wysyłanie powiadomień pocztowych wg harmonogramu.

Wysyłanie powiadomień pocztowych wg harmonogramu może być ustawione w 30-to minutowych odstępach czasowych.

Delay of occasional e-mails – Opóźnienie wysyłania incydentalnych e-maili

Za pomocą tego parametru możesz ustawić, jakie będzie opóźnienie pomiędzy wystąpieniem zdarzenia a wysłaniem powiadomienia.

Internal tables – Wewnętrzne tablice

Możesz ustawić wielkość wewnętrznych tablic programu VirusBuster for NetWare Servers. Wielkość tablic jest podawana w bajtach. Mogą być ustawione następujące wielkości tablic:

- On-access file cache size (Wielkość pamięci podręcznej w trybie bezpośredniego dostępu): Program przechowuje w tej tablicy nazwy plików, które zostały uznane za pozbawione wirusów podczas skanowania w trybie dostępu. W przypadku ponownego dostępu plik nie będzie sprawdzany, jeśli znajduje się w tej tablicy. W przypadku zapisu nazwa pliku zostanie

automatycznie usunięta z tablicy. Jeśli nie chcesz skorzystać z tej opcji ustaw wielkość pamięci podręcznej na 0.

- Redirection table: Wielkość tablicy przekierowania.
- Domain table: wielkość tablicy przechowującej informację o chronionych domenach.

Quarantine - Kwarantanna

Zadaniem kwarantanny jest przechowywanie zarażonych lub podejrzanych plików i zarządzanie nimi zgodnie z ustawieniami użytkownika.

Jeżeli wskażesz pozycję kwarantanny otrzymasz informacje na temat wybranego pliku w nowym oknie i będziesz mógł wybrać, co z nim zrobić używając *Quarantine actions* z menu.

- Keep (zachowaj bez zmian): program zachowuje plik bez zmian.
- Save as (zachowaj jako): program zachowuje pliki w postaci zakodowanej i mogą być one wysyłane do analizy.
- Delete (usuń): program usuwa wybrany plik nieodwracalnie.
- Rescan (ponowne skanowanie): program skanuje plik i jeżeli to możliwe usuwa wirusy.
- Restore (przywrócenie pliku): program przywraca plik w poprzedniej lokalizacji i jeśli podana ścieżka istnieje i jeżeli nie istnieje inny plik o tej samej nazwie w tej samej lokalizacji.

Działania te zostaną wykonane po zamknięciu okna!

Information - Informacje

W tym menu uzyskasz informacje o programie.

About - Informacje o programie

Zawiera adresy, telefony i inne niezbędne informacje dotyczące dystrybutora i wsparcia technicznego a także wersji programu. Można w tym miejscu sprawdzić status silnika skanowania (załadowany lub nie).

Runtime options – Ustawienia uruchamiania

Możliwe są następujące opcje:

- Start scanning (uruchom skanowanie): wyświetla listę domen gdzie skanowanie może zostać wykonane (aktualnie skanowanie nie odbywa się a zapis domeny jest poprawny). Skanowanie rozpoczyna się po zaznaczeniu domeny lub kilku domen.
- Stop scanning (zatrzymaj skanowanie): wyświetla listę domen gdzie skanowanie jest aktualnie uruchomione (manualnie lub wynikające z harmonogramu). W tym drugim przypadku, nazwa domeny znajduje się w nawiasach. Po wskazaniu domeny skanowanie zostanie przerwane.
- Report file listing (lista raportów): pokazuje listę zapisanych plików, które mogą być wyświetlone. Po wskazaniu pliku, program wyświetli jego zawartość. Jeśli plik jest większy niż jeden ekran, program przełączy się w tryb umożliwiający pokazywanie kolejnych wpisów automatycznie.

Registration - Rejestracja

Możesz uruchomić program, jeśli posiadasz nazwę użytkownika i poprawny klucz licencyjny do programu

Based on the VirusBuster's registration policy, the purchased VirusBuster product version can be used as long as the user wants to without any restriction. So, the purchased license has not time limit, if the

registration has expired the current product version can be used for any length of time. But if any of the program components is updated after expiring, the program cannot be started anymore (user needs to renew the license to use the product again). The update restriction does not affect the database updates, these files can be updated without any consequence at any time – even the registration has expired (but we cannot guarantee the continual compatibility).

After the registration has expired the product stops the automatic program update so that it doesn't have to terminate its operation because of the new (updated) program modules. When it is happening, the product is notifying the user by a message window (and log record) which is displayed every time the user tries to start a manual update. If the registration has expired, the update of the program modules is not allowed. After renewing the license, the program automatically reset the module update settings to the former status.

```
Registration
Registered: 8
User: TEST
Key: WEW43-TG64G-TTR6B
Registration will expire soon: 2005. 2. 4.
```

Okno rejestracji

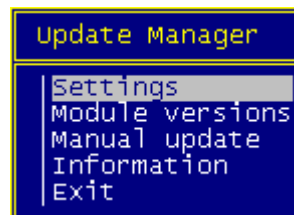
Registration process – proces rejestracji

Podczas procesu rejestracji użytkownik otrzyma klucz licencyjny z nazwą i liczbą użytkowników. Nazwa i klucz licencyjny może być wprowadzona po wybraniu z menu *Global Options/Registration*. Pojawi się okno zawierające status rejestracji, liczbę użytkowników jak i liczbę zarejestrowanych użytkowników.

- ! Uwaga!
- | Uważaj na małe i wielkie litery podczas wprowadzania danych licencyjnych!

UPDATE MANAGER – Menedżer aktualizacji

Program VirusBuster oparty na cechach systemu Novell można bez problemu aktualizować korzystając z pomocy *Update Manager*. Aby zainstalować moduł updater (aktualizacja) z płyty instalacyjnej skopiuj pliki **VBUPDATE.NLM**, **VBUPDASC.NLM** oraz plik **VBUSTER.INI** jeżeli jeszcze nie istnieją do katalogu VirusBuster for NetWare Servers. Aktualizacja zostanie rozpoczęta po użyciu komendy **load vbupdate**. W oknie konsoli są wyświetlone następujące opcje:



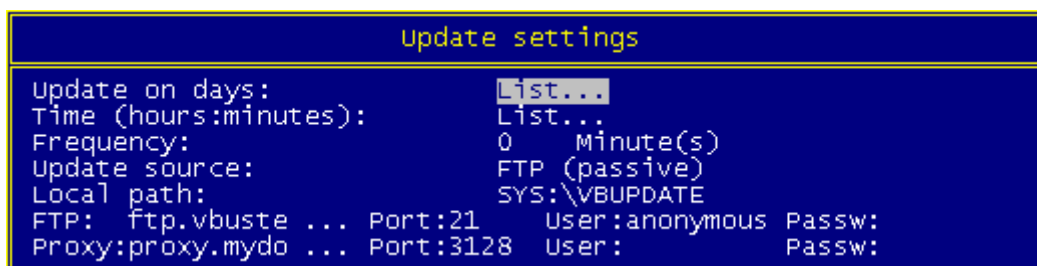
Menu główne menedżera aktualizacji

Produkt używa przyrostowy mechanizm uaktualniając na bieżąco bazę danych sygnatur. Jest to korzystne dlatego, że nie musimy ściągać za każdym razem całej bazy sygnatur (zwykle zajmuje kilka MB) tylko zazwyczaj mały dodany pakiet zawierający sygnatury ostatnio wypuszczonych wirusów. Dzięki temu mechanizmowi czas potrzebny na aktualizację jest minimalnie skrócony, co pozwala publikować po kilka aktualizacji baz sygnatur dziennie. To wydatnie podnosi ochronę. Użytkownik może otrzymać ochronę na nowe MALWERS'Y bez spędzania długiego czasu i generowania obciążania sieci na uaktualnianie. Ochrona jest dostępna niemalże natychmiastowo po opracowaniu w naszych laboratoriach sygnatur nowo odkrytego wirusa.

Settings - Ustawienia

Ogólne ustawienia dotyczące zarówno automatycznej, jak i manualnej aktualizacji są pokazane w tym oknie.

By the default update setting, the product tries to update the program- and database modules by two hours to keep the protection up-to-date.



Ustawienia aktualizacji

Update on days – aktualizacja w dniach

Za pomocą tej opcji możesz określić, w jakich dniach będzie aktualizowany program. Przy pomocy klawisza **Insert** mogą zostać dodane nowe dni a za pomocą klawisza **Delete** można usunąć dni występujące na liście.

Time - czas

Lista ta podaje czas, kiedy program powinien być aktualizowany. Czas musi być podany w 24h formacie

godzina:minuta. Określona wartość jest ważna, kiedy wartość 0 (zero) jest podana w następnej pozycji menu (Frequency).

Frequency - częstotliwość

Częstotliwość aktualizacji może być podana w minutach. Program wykonuje aktualizację, co określoną liczbę minut, jeśli opcja ta jest włączona.

Update source – Źródło aktualizacji

Tutaj może zostać określony typ źródła, z którego program pobiera aktualizację. Może zostać określony adres lokalnej ścieżki, pasywne lub aktywne połączenie FTP albo połączenie FTP realizowane poprzez Proxy FTP.

Local path – ścieżka lokalna

Tutaj możesz wprowadzić ścieżkę do serwera gdzie znajdują się pakiety instalacyjne.

FTP/Port/User name/Password – FTP/Port/Nazwa użytkownika/Hasło

Tutaj możesz wprowadzić dane serwera FTP. Sugerujemy użycie domyślnych ustawień; dla nazwy serwera update.virusbuster.hu/pub12 używając portu 21 jako użytkownik *anonymous* bez podania hasła.

Proxy/Port/User name/Password – Proxy/Port/ Nazwa użytkownika/hasło

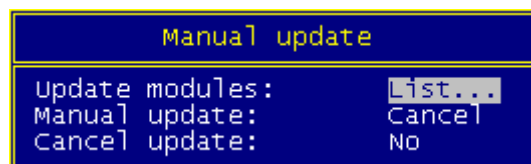
Pola te powinny być wypełnione jeśli aktualizacja FTP została wykonana poprzez serwer FTP Proxy. Domyślnie proponujemy użyć portu 3128.

Module versions – wersje modułów

Tutaj wyświetlone są wersje modułów programu i daty ich utworzenia. Możesz także wskazać tutaj, jakie moduły będą aktualizowane. Pod nazwą produktu możesz obejrzeć konkretne moduły z nim związane, a także ich wersje i daty utworzenia. Kolejne pole to przełącznik określający, czy aktualizować moduł czy też nie.

Manual update – aktualizacja manualna

Aktualizacja manualna może być wykonana w tym oknie:



Manualna aktualizacja

Update modules – aktualizacja modułów

Lista ta zawiera wszystkie moduły, jakie mogą być odnawiane podczas procesu aktualizacji. Moduły wymienione tutaj są tymi, które zostały wybrane do aktualizacji w oknie Module versions.

Manual update – aktualizacja manualna

Ten parametr pozwala uruchomić proces aktualizacji poprzez wybór opcji Start. Proces aktualizacji zostanie rozpoczęty tylko wtedy, gdy nie jest uruchomione żadne inne zadanie!

Cancel update – anulowanie aktualizacji

Za pomocą tej opcji uruchomiony proces aktualizacji może zostać przerwany (anulowany).

Information – Informacje

Tu możesz odczytać informacje o producencie i adres firmy VirusBuster Ltd.

END USER AGREEMENT

THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU AND VirusBuster Ltd. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY INSTALLING AND USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS THEN DO NOT INSTALL THE SOFTWARE.

IMPORTANT NOTICE TO USERS: THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

1. Definitions

- (a) "Educational Version" means a version of the Software, so identified, for use by students and faculty of educational institutions only. "Home version" means a version of the Software, so identified, for use by individuals on a single computer at home only. Educational and Home Versions may not be used for, or distributed to any party for, any commercial purpose.*
- (b) Henceforward VirusBuster Ltd. means VirusBuster Ltd. and (where interpretable) its suppliers and licensors, if any.*
- (c) "Not For Resale (NFR) Version" means a version of the Software, so identified, to be used to review and evaluate the Software, only.*
- (d) "Software" means the VirusBuster Ltd. (R) VirusBuster(TM) software program supplied by VirusBuster Ltd. herewith, which may also include documentation, associated media, printed materials, and online and electronic documentation.*

2. License

This EULA allows you to:

- (a) Install and use the Software on a single computer; OR install and store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network, provided you have a license for each separate computer on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers.*
- (b) Educational and Home Version Only. If you have purchased a license for the Educational and/or the Home Version of the Software, then you may install or store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network for use by a total number of concurrent users not to exceed the number of user licenses you have been granted; provided, you agree to implement reasonable controls to ensure that your use of the Software does not exceed the number of licenses you have been granted. You agree that VirusBuster Ltd. may audit your use of the Software for compliance with the EULA at any time, upon reasonable notice.*
- (c) Make one copy of the Software in machine-readable form solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software.*

3. License Restrictions

- (a) Other than as set forth in Section 2, you may not make or distribute copies of the Software, or electronically transfer the Software from one computer to another or over a network.*
- (b) You may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.*
- (c) You may not sell, rent, lease, transfer or sublicense the Software.*
- (d) You may not modify the Software or create derivative works based upon the Software.*
- (e) You may not use the Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.*
- (f) In the event that you fail to comply with this EULA, VirusBuster Ltd. may terminate the license and you must destroy all copies of the Software.*

4. Upgrades

If this copy of the Software is an upgrade from an earlier version of the Software, it is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your earlier EULA and that you will not continue to use the earlier version of the Software or transfer it to another person or entity.

5. Ownership

The foregoing license gives you limited rights to use the Software. VirusBuster Ltd. and its suppliers retain all right, title and interest, including all copyrights, in and to the Software and all copies thereof. All rights not specifically granted in this EULA, including International Copyrights, are reserved by VirusBuster Ltd. and its suppliers.

6. LIMITED WARRANTY AND DISCLAIMER

- (a) LIMITED WARRANTY. VirusBuster Ltd. warrants that, for a period of ninety (90) days from the date of delivery (as*

evidenced by a copy of your receipt) that the physical media on which the Software is furnished will be free from defects in materials and workmanship under normal use.

(b) NO OTHER WARRANTY. EXCEPT AS SET FORTH IN THE FOREGOING LIMITED WARRANTY, VirusBuster Ltd. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, OR OTHERWISE INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NONINFRINGEMENT, TITLE OR QUIET ENJOYMENT. IF APPLICABLE LAW IMPLIES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCH WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY. No verbal or written information or advice given by VirusBuster Ltd. its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of this warranty.

7. Exclusive Remedy

Your exclusive remedy under Section 6 is to return the Software to the place you acquired it, with a copy of your receipt and a description of the problem. VirusBuster Ltd. will use reasonable commercial efforts to supply you with a replacement copy of the Software that substantially conforms to the documentation, provide a replacement for defective media. VirusBuster Ltd. shall have no responsibility if the Software has been altered in any way, if the media has been damaged by accident, abuse or misapplication, or if the failure arises out of use of the Software with other than a recommended hardware configuration.

8. LIMITATION OF LIABILITY.

NEITHER VirusBuster Ltd. NOR ITS SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR THIS EULA BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF VirusBuster Ltd. OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

9. Basis of Bargain

The Limited Warranty, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between VirusBuster Ltd. and you. VirusBuster Ltd. would not be able to provide the Software on an economic basis without such limitations.

10. Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business.

11. General Provisions

The internal laws of Hungary shall govern this EULA. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. All questions concerning this EULA shall be directed to VirusBuster Ltd.

VirusBuster and VirusBuster logo are trademarks or registered trademarks of VirusBuster Ltd. in Hungary and/or other countries. Other marks are the properties of their respective owners.

CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address VirusBuster Ltd.
Budapest 1518,
Pf. 54.
Hungary

Phone (+36) 1 382-7000
Fax (+36) 1 382-7007
Web <http://www.virusbuster.hu>
Support <https://support.virusbuster.hu>
E-mail sales@virusbuster.hu
support@virusbuster.hu