Dr.WEB®
Antywirus

Chroń to, co tworzysz

Linia produktów Dr.Web® Security Suite

Instrukcja udzielania licencji

Treść

O firmie „Doctor Web” ... 4
Technologie Dr.Web ... 4
Licencje i certyfikaty ... 9
Certyfikat licencyjny Dr.Web ... 10
Linia produktów Dr.Web Security Suite ... 11
Licencjonowanie produktów Dr.Web ... 11
Rodzaje dostawy produktów Dr.Web ... 13
Dr.Web Home Security Suite – produkty dla użytkowników domowych ... 17
Dr.Web Security Space ... 17
Antywirus Dr.Web dla Windows ... 21
Antywirus Dr.Web dla Mac OS X ... 24
Antywirus Dr.Web dla Linux ... 25
Skanery konsolowe Dr.Web ... 26
„Dr.Web Uniwersalny” (dla klientów ACS) ... 26
Dr.Web Enterprise Security Suite. Produkty dla przedsiębiorstw ... 27
Centrum zarządzania Dr.Web ... 28
Dr.Web Desktop Security Suite ... 31
Dr.Web Server Security Suite ... 32
Dr.Web dla serwerów Windows ... 32
Dr.Web dla Mac OS X Server ... 34
Dr.Web dla serwerów Novell NetWare ... 35
Dr.Web dla serwerów Unix ... 36
Dr.Web dla Novell Storage Services ... 37
Dr.Web Mail Security Suite ... 38
Dr.Web dla serwerów pocztowych i bram Unix ... 40
Dr.Web dla MS Exchange ... 43
Dr.Web dla IBM Lotus Domino ... 45
Dr.Web dla serwerów pocztowych Kerio ... 46
Dr.Web Gateway Security Suite ... 47
Dr.Web dla bram internetowych Unix ... 48
Dr.Web dla bram internetowych Kerio ... 49
Dr.Web dla MIMEsweeper ... 50
Dr.Web dla Qbik WinGate ... 51
Dr.Web Mobile Security Suite ... 52
Dr.Web Retail Security Suite. Produkty dla klientów detalicznych ... 54

24.07.2013

„Dr.Web Uniwersalny" (dla klientów ACS) ... 55
Zestawy Dr.Web ... 55
Narzędzia ... 56
Zestawy programowo-sprzętowe Dr.Web Office Shield ... 58
Rozwiązania ... 61
Dr.Web Security Suite dla Unix Appliance ... 61
Dr.Web ATM Shield ... 61
Serwisy ... 63
Polityka rabatów ... 65
Ogólne warunki sprzedaży ... 66
Kody produktów, zestawów, narzędzi i zestawów programowo-sprzętowych Dr.Web ... 68
Kontakty ... 71

O firmie „Doctor Web"

Firma „Doctor Web" to znany rosyjski producent narzędzi bezpieczeństwa informacyjnego.

Programy antywirusowe Dr.Web, opracowywane od 1992 roku, osiągają niezmiennie doskonałe wyniki w wykrywaniu złośliwego oprogramowania. Utworzenie firmy „Doctor Web" w grudniu 2003 roku zapoczątkowało gwałtowny wzrost sprzedaży produktów Dr.Web zarówno w Rosji, jak i w innych krajach.

Dzisiaj „Doctor Web" to odnosząca sukcesy, szybko rozwijająca się firma, która odgrywa rolę jednego z liderów na rynku produktów bezpieczeństwa informacyjnego. Dysponuje silnikiem antywirusowym własnego autorstwa, posiada własne laboratorium antywirusowe, globalny serwis monitorowania wirusów i serwis wsparcia technicznego.

Strategicznym zadaniem firmy, którego wykonanie jest celem starań wszystkich pracowników, jest stworzenie produktów ochrony antywirusowej, odpowiadających wszystkim aktualnym wymaganiom. Nie mniej ważne jest opracowanie nowych rozwiązań technologicznych, dzięki którym użytkownicy będą w pełni przygotowani na wszelkiego rodzaju zagrożenia komputerowe. Linia produktów antywirusowych firmy „Doctor Web" obejmuje najszerszy zakres systemów operacyjnych i kompatybilnych aplikacji.

Firma rozprowadza swoje opracowania w oparciu o sieć partnerską, rezygnując ze sprzedaży bezpośredniej końcowym użytkownikom.

Z produktów Dr.Web korzystają domowi użytkownicy z różnych krajów świata, przedsiębiorstwa, instytucje państwowe, niewielkie organizacje i duże strategiczne korporacje, którym zespół „Doctor Web" jest wdzięczny za wsparcie i długoletnią wierność produktowi. Certyfikaty i nagrody państwowe świadczą o dużym zaufaniu do programu antywirusowego Dr.Web, stworzonego przez utalentowanych rosyjskich programistów.

Technologie Dr.Web

Programy antywirusowe Dr.Web to rodzina programów komputerowych, stworzonych przez rosyjskich programistów pod kierunkiem Igora Daniłowa.

„Doctor Web" to jeden z nielicznych dostawców programów antywirusowych na świecie, posiadających własną unikalną technologię wykrywania i leczenia złośliwego oprogramowania. Firma posiada własny serwis monitorowania wirusów i laboratorium analityczne. Dzięki temu specjaliści mogą szybko zareagować na nowe zagrożenia wirusowe i są zdolni pomóc klientom w rozwiązywaniu problemów o dowolnej złożoności w kilka godzin.

Istotną właściwością Dr.Web jest jego modułowa architektura. Wszystkie produkty i rozwiązania zawierają w sobie ten sam silnik antywirusowy, a także wykorzystują ten sam system aktualizacji baz wirusów i globalny system wsparcia technicznego. Technologie Dr.Web pozwalają stworzyć niezawodną ochronę informacyjną, zarówno w ramach dużych sieci korporacyjnych, jak i w domowym komputerze czy też domowym biurze.

Oprócz wirusów i złośliwego oprogramowania, Dr.Web potrafi również wykrywać i usuwać z komputera różnego rodzaju niechciane programy (programy reklamowe, dialery, programy–żarty, programy potencjalnie niebezpieczne, programy do włamań – spyware / riskware), spam i niechciane listy elektroniczne (wiadomości typu phishing, pharming, scamming i bounce).

Technologie

Dobrej jakości antywirus powinien umieć nie tylko wykrywać wirusy, ale i je leczyć. Czym innym przecież jest usunięcie zainfekowanych plików razem z ich cenną informacją, a czym innym przywrócenie ich do pierwotnego „zdrowego" stanu. Dr.Web ostrożnie obchodzi się z plikami użytkownika.

Leczy z wirusów

- Dr.Web w odróżnieniu od wszystkich innych analogicznych programów z powodzeniem działa na komputerze już zainfekowanym i jest niepokonany w walce z wirusami.
- W całej branży antywirusowej Dr.Web charakteryzuje się najwyższym odsetkiem skutecznego leczenia aktywnych infekcji.
- Nie ma potrzeby wstępnego leczenia PC przed instalacją Dr.Web: wykorzystanie unikalnych technologii do obróbki procesów w pamięci oraz doskonałe możliwości w zakresie neutralizacji aktywnych infekcji, pozwalają zainstalować Dr.Web bezpośrednio na zainfekowanym komputerze.
- Wysokie prawdopodobieństwo pomyślnego uruchomienia skanowania zainfekowanego PC – nawet z zewnętrznego nośnika bez instalacji do systemu (np. z pamięci USB).

Samoochrona

Dr.Web jest bardzo wytrzymały na wszelkie próby uszkodzenia go przez złośliwe oprogramowania. Jest niepokonany, co zawdzięcza bezkonkurencyjnemu na rynku antywirusów komponentowi samoochrony Dr.Web SelfPROtect.

- Dr.Web SelfPROtect wykonany jest w formie sterownika i działa na najniższym poziomie systemowym – jego pracę może przerwać jedynie ponowne uruchomienie systemu. W ten sposób złośliwe programy nie mogą wpływać na samoochronę.
- Dr.Web SelfPROtect ogranicza dostęp złośliwych obiektów do sieci, plików i katalogów, niektórych gałęzi rejestru oraz nośników wymiennych na poziomie sterownika systemowego, chroni przed próbami zakończenia pracy Dr.Web przez programy anty-antywirusowe.
- Dr.Web SelfPROtect jest w pełni samowystarczalny i nie modyfikuje jądra Windows, podczas gdy niektóre produkty konkurencyjne przechwytują przerwania, zamieniają tablice wektorowe, korzystają z nieudokumentowanych funkcji itp., co może doprowadzić do poważnych problemów w pracy samego systemu operacyjnego, a także daje przestępcom internetowym nowe możliwości wykorzystywania braku zabezpieczenia.
- Możliwość automatycznej odbudowy własnych modułów.

Unikalne możliwości jądra

- Skanowanie archiwów o dowolnym poziome zagnieżdżenia.
- Najwyższa dokładność w wykrywaniu spakowanych obiektów złośliwych (nawet tych, które spakowane są metodą nieznaną dla Dr.Web) - rozpakowanie ich na składniki i szczegółowa analiza w celu wykrycia ukrytych zagrożeń.
- Wykrywanie i neutralizacja skomplikowanych wirusów.
- Inteligentne technologie skanowania pamięci pozwalają na blokowanie aktywnych wirusów do momentu pojawienia się ich kopii na dysku twardym komputera, co zmniejsza prawdopodobieństwo wykorzystania przez złośliwe oprogramowanie braku zabezpieczenia zainstalowanych programów lub systemu operacyjnego.
- Wykrywanie i neutralizacja wirusów, które działają w pamięci operacyjnej i nigdy nie występują w formie oddzielnych plików (np. Slammer i CodeRed).

Walka z nieznanymi zagrożeniami

- FLY-CODE to bezkonkurencyjna technologia uniwersalnego rozpakowywania plików, spakowanych za pomocą nieznanych dla Dr.Web metod.
- Unikalna technologia bezsygnaturowego wykrywania OriginsTracing™ pozwala Dr.Web z dużym prawdopodobieństwem rozpoznawać złośliwe programy, zanim te zostaną wpisane do jego bazy wirusów.
- Heurystyczny analizator Dr.Web skutecznie wykrywa wszystkie rozpowszechnione typy zagrożeń, określając ich klasę na podstawie wyników przeprowadzonej analizy i po znakach szczególnych.

Technologie filtrowania spamu

Technologie filtrowania spamu Dr.Web składają się z kilku tysięcy reguł, które umownie można podzielić na kilka grup.

Analiza heurystyczna

Niezwykle skomplikowana, wysoce inteligentna technologia empirycznej analizy wszystkich części wiadomości: pola nagłówka, treści wiadomości, itd. Analizie poddawana jest nie tylko sama wiadomość, ale i treść załączników do niej, jeżeli takie występują. Heurystyczny analizator jest stale udoskonalany i ciągle uzupełniany o nowe reguły. Analizator heurystyczny pracuje „z wyprzedzeniem" i umożliwia rozpoznawanie nieznanych jeszcze odmian spamu nowej generacji przed wydaniem odpowiedniej aktualizacji.

Filtrowanie przeciwdziałania

Filtrowanie przeciwdziałania to jedna z czołowych i najbardziej skutecznych technologii antyspamowych Dr.Web. Polega na rozpoznaniu trików stosowanych przez spamerów w celu obejścia filtrów antyspamowych.

Analiza na bazie sygnatur HTML

Wiadomości, w skład których wchodzi kod HTML, porównywane są z wzorcami biblioteki sygnatur HTML antyspamu. Takie porównanie, w połączeniu z dostępnymi informacjami o wielkości stosowanych zwykle przez spamerów obrazków, chroni użytkowników przed wiadomościami spamowymi z kodem HTML, do których często zalicza się obrazki on-line.

Technologia wykrywania spamu po kopertach wiadomości

Wykrywanie fałszywek w „stemplach" serwerów SMTP i w innych elementach, jakie umieszczone są w nagłówkach wiadomości pocztowych, to najnowszy kierunek rozwoju metod walki ze spamem. Nie wolno ufać adresowi nadawcy wiadomości elektronicznej, gdyż może być tam podany fałszywy adres zwrotny. Fałszywe listy to nie tylko spam, mogą to być również mistyfikacje lub środki nacisku na personel, na przykład anonimy, a nawet groźby. Specjalne technologie antyspamu Dr.Web pozwa-lają ustalić fałszywe adresy i nie odbierać takich wiadomości. Dzięki temu możemy zmniejszyć ruch w sieci i uchronić pracowników przed otrzymywaniem fałszywych listów, które mogłyby ich skłonić do nieprzewidywalnych czynności.

Analiza semantyczna

W trakcie tej analizy porównuje się słowa i zwroty wiadomości ze słowami i idiomami, zwykle stosowanymi w spamie. Porównania dokonuje się na podstawie specjalnego słownika, przy czym analizie poddawane są słowa, zwroty i symbole, zarówno widoczne dla ludzkiego oka, jak i te zamaskowane specjalnymi technikami.

Technologia Anti-Scamming

Wiadomości typu scam (jak również wiadomości typu pharming – jeden z rodzajów scammingu) – to chyba najgroźniejszy rodzaj wiadomości spamowych, do których zalicza się tzw. „listy nigeryjskie", wiadomości o wygranych w loteriach, kasynie, fałszywe listy bankowe i od instytucji kredytowych. Antyspam Dr.Web został wyposażony w specjalny moduł do ich filtracji.

Filtrowanie spamu technicznego

Tak zwane wiadomości bounce powstają jako reakcja na wirusy lub jako przejaw aktywności wirusów – na przykład w wyniku działania robaka pocztowego, rozsyłającego listy, lub w formie wiadomości o niedostarczeniu listu – i są równie niepożądane co spam. Specjalny moduł antyspamowy Dr.Web określa takie wiadomości jako niepożądane.

Zalety Antyspamu Dr.Web

- Skanowanie poczty przychodzącej i wychodzącej następuje w czasie rzeczywistym.
- Praca antyspamu nie jest zależna od użytkowanego programu pocztowego i nie wydłuża czasu odbioru poczty.
- Antyspam nie wymaga konfigurowania, zaczyna działać automatycznie wraz z odbiorem pierwszej wiadomości.
- Różne technologie filtracji gwarantują duże prawdopodobieństwo rozpoznania spamu oraz wiadomości typu phishing, pharming, scamming i bounce, przy prawie zerowym odsetku błędnej kwalifikacji.
- Przefiltrowane listy nie są usuwane, lecz przenoszone do specjalnego katalogu programu pocztowego, w którym w dogodnym terminie można sprawdzić, czy nie zostały mylnie zakwalifikowane.
- Moduł analizatora spamu jest całkowicie niezależny; nie trzeba go łączyć z zewnętrznym serwerem, nie wymaga też dostępu do jakiejkolwiek bazy danych, a to pozwala istotnie zmniejszyć ruch w sieci.
- Aktualizacje dla antyspamu Dr.Web pojawiają się codziennie. Dzięki unikalnym technologiom rozpoznawania niechcianej poczty, w oparciu o kilka tysięcy reguł, aktualizacji nie trzeba przeprowadzać częściej niż jeden raz na dobę, co pozwala zmniejszyć ruch w sieci.

Szczególna organizacja bazy wirusów Dr.Web

Wielkość bazy wirusów Dr.Web jest najmniejsza ze wszystkich istniejących baz innych programów antywirusowych. Osiągnięcie takiego stanu było możliwe dzięki własnej technologii tworzenia bazy wirusów w oparciu o niezwykle elastyczny język, specjalnie opracowany dla opisywania baz. Niewielki rozmiar bazy wirusów daje możliwość zmniejszenia ruchu w sieci, umożliwia zajęcie przez nią znacznie mniej miejsca na dysku po instalacji oraz w pamięci operacyjnej, niż bazy innych producentów. Niewielki rozmiar bazy wirusów pozwala współpracować komponentom programu Dr.Web w bardzo szybkim czasie, nie obciążając nadmiernie procesora.

Jakie jest najważniejsze zadanie programu antywirusowego? Zapewnić ochronę przed wirusami. Ochrona jest zapewniona, między innymi, poprzez wprowadzenie do bazy wirusów zapisów (sygnatur), pozwalających na wykrycie wirusów. Liczba zapisów w bazie wirusów wcale nie świadczy o tym, ile wirusów realnie wychwytuje dany program antywirusowy. Aby zrozumieć, dlaczego liczba zapisów w bazie wirusów Dr.Web jest mniejsza od liczby zapisów w bazach wirusów niektórych innych producentów, trzeba wiedzieć, że nie wszystkie wirusy są unikalne. Istnieją całe rodziny spokrewnionych (podobnych) wirusów, są też wirusy stworzone przez konstruktorów wirusów. Dla każdego takiego wirusa-bliźniaka twórcy niektórych innych antywirusów robią oddzielny zapis w bazie wirusów, zwiększając jej ciężar. Inną regułę stosuje się w bazie wirusów Dr.Web, gdzie wystarczy jeden zapis, by unieszkodliwić dziesiątki czy też setki, a czasem i tysiące podobnych do siebie wirusów.

Zalety bazy wirusów Dr.Web

- Rekordowo mała liczba zapisów.
- Niewielki rozmiar aktualizacji.
- Wystarczy jeden zapis, by określić dziesiątki, setki, a nawet tysiące podobnych wirusów.

Zasadnicza różnica między bazą wirusów Dr.Web a bazami wielu innych programów polega na tym, że przy mniejszej liczbie zapisów pozwala ona wykrywać tyle samo (a nawet jeszcze więcej) wirusów i złośliwego oprogramowania.

Jakie korzyści daje użytkownikowi niewielki rozmiar bazy Dr.Web i mniejsza liczba zapisów w tej bazie?

- Oszczędność miejsca na dysku.
- Oszczędność pamięci operacyjnej.
- Zmniejszenie ruchu w sieci przy ściąganiu bazy.
- Duża prędkość instalacji bazy i jej obsługi przy analizie wirusów.
- Możliwość identyfikacji wirusów, które będą stworzone dopiero w przyszłości poprzez modyfikację już znanych wirusów.

Globalny system aktualizacji Dr.Web (Dr.Web GUS)

- Serwis monitorowania wirusów Dr.Web zbiera wzorce wirusów na całym świecie.
- Najnowsze aktualizacje pojawiają się natychmiast po dokonaniu analizy nowego zagrożenia wirusowego i przygotowaniu aktualizacji.
- Zanim aktualizacje będą dostępne użytkownikom, są testowane na ogromnej liczbie „zdrowych" plików.
- Aktualizacje trafiają do użytkowników z kilku serwerów, znajdujących się w różnych miejscach na kuli ziemskiej, co minimalizuje czas ich uzyskania.
- Proces aktualizacji baz wirusów i modułów programowych jest w pełni zautomatyzowany.
- Aktualizacje można pobierać w formie zarchiwizowanych plików.

Licencje i certyfikaty

W odróżnieniu od większości rozwiązań konkurencji, produkty programowe Dr.Web posiadają certyfikaty zgodności Federalnej Służby Kontroli Technicznej i Eksportowej (FSKTiE), Federalnej Służby Bezpieczeństwa (FSB) i Ministerstwa Obrony Federacji Rosyjskiej. Dzięki temu mogą je wykorzystywać organizacje o podwyższonych wymaganiach dotyczących poziomu bezpieczeństwa.

Dr.Web został certyfikowany przez FSKTiE na zgodność:

- WT (warunki techniczne) i NDW 4 (niezadeklarowane możliwości) na zastosowanie w składzie podsystemu ochrony antywirusowej w systemach informatycznych danych osobowych (SIDO) klasy K1;
- z wymaganiami (nie niżej niż 4 poziom kontroli) dokumentu wiodącego Państwowej Komisji Technicznej Rosji „Ochrona przed nieautoryzowanym dostępem do informacji. Część 1. Zabezpieczenie programowe środków ochrony informacji. Klasyfikacja poziomu kontroli braku niezadeklarowanych możliwości" i z wymaganiami warunków technicznych.

Dr.Web całkowicie spełnia wymagania ustawy o danych osobowych, jakie stawia się produktom antywirusowym w zakresie ochrony przed nieautoryzowanym dostępem oraz scentralizowanej ochrony kanałów przekazu danych, i może być używany w sieciach, odpowiadających maksymalnemu poziomowi ochrony.

Firma „Doctor Web" ma następujące licencje, certyfikaty i świadectwa:

- licencje Federalnej Służby Kontroli Technicznej i Eksportowej FR (FSKTiE) na prowadzenie prac, związanych z tworzeniem środków ochrony informacji, a także na działalność dotyczącą opracowania i/lub produkcji środków ochrony informacji poufnej;
- licencja Ministerstwa Obrony Federacji Rosyjskiej na działalność w zakresie tworzenia środków ochrony informacji;
- licencje FSB Rosji na prowadzenie prac związanych z wykorzystaniem informacji, będących tajemnicą państwową;
- licencja Centrum Licencjonowania, Certyfikacji i Ochrony Tajemnicy Państwowej FSB Rosji na opracowanie i/lub produkcję środków ochrony informacji poufnej;
- certyfikaty zgodności FSB FR;
- certyfikaty zgodności FSKTiE FR.

Wszystkie licencje i certyfikaty „Doctor Web":

http://company.drweb.com/licenses_and_certificates

Opakowanie produktów certyfikowanych przez FSKTiE

Specjalny pakiet medialny „Dr.Web Certyfikowany"

Kompletowanie:

- Pakiet medialny
- Dysk (dostarczany z certyfikowanym produktem)
- Formularz
- Naklejka holograficzna FSKTiE

Certyfikat licencyjny Dr.Web


CERTYFIKAT
autentyczności

Dr.WEB®

certyfikat ten jest zaświadczeniem, że oprogramowanie jest prawnie licencjonowane przez firmę **Doctor Web** – producenta oraz właściciela produktów bezpieczeństwa **Dr.WEB®**.

Nabywca licencji

Licencjonowany produkt

Numer seryjny

Numer seryjny

Numer seryjny

Chronione obiekty

Stacje robocze	Serwery
Poczta elektroniczna	Bramy internetowe
Urządzenia mobilne	Centrum zarządzania

Termin ważności licencji

Pośrednik sprzedaży

Boris Sharov, CEO
Doctor Web Ltd.

«Доктор Веб»
«Doctor Web», Ltd.

Certyfikat licencyjny Dr.Web to dokument, potwierdzający legalność korzystania z oprogramowania Dr.Web dla organów kontrolnych.

WAŻNE! Certyfikat licencyjny Dr.Web nie stanowi podstawy przedłużenia licencji i otrzymania rabatu na przedłużenie.

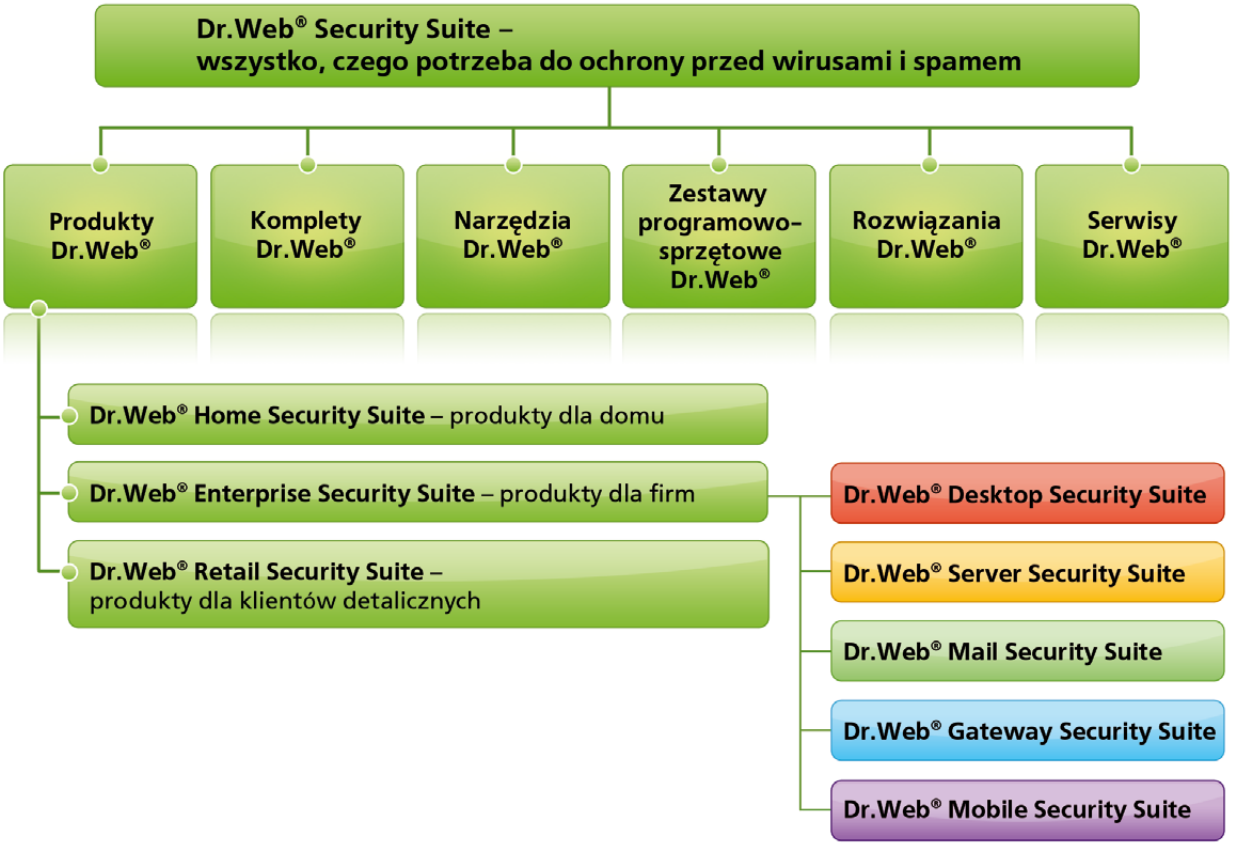
Certyfikat posiada wysoki stopień ochrony. Dzięki specjalnej giloszowanej siatce jego podrobienie jest niemożliwe.

Dostawa blankietu certyfikatu licencyjnego wraz z dowolnymi produktami Dr.Web dla osób prawnych jest obowiązkowa!

Kopię elektroniczną certyfikatu licencyjnego Dr.Web można wygenerować samodzielnie na stronie http://products.drweb.com/register/certificate/.

Linia produktów Dr.Web Security Suite

Linia produktów Dr.Web Security Suite składa się z produktów komercyjnych dla domu, przedsiębiorstw i klientów detalicznych, kompletów, narzędzi, zestawów programowo-sprzętowych, rozwiązań i serwisów.



Licencjonowanie produktów Dr.Web

1. Licencje na produkty Dr.Web® przyznawane są na 12, 24 i 36 miesięcy. Dla Dr.Web Security Space i Antywirus Dr.Web dla Windows licencje przyznawane są również na 3 i 6 miesięcy.
2. Produkty Dr.Web są licencjonowane zależnie od rodzaju obiektów, które chronią.
3. Chronione obiekty obejmują:
   - stacje robocze, klientów serwerów terminalowych i klientów systemów wbudowanych;
   - serwery plików i serwery aplikacji (w tym serwery terminalowe);
   - użytkowników poczty;
   - użytkowników bram pocztowych i internetowych;
   - urządzenia mobilne.

4. Przewidziano 2 typy **licencji bazowych**:
   1) Antywirus (z zaporą sieciową firewall);
   2) Ochrona kompleksowa (z zaporą sieciową firewall).
5. Licencja bazowa Ochrona kompleksowa jest przeznaczona tylko dla produktów do ochrony stacji roboczych.
6. W skład licencji Ochrona kompleksowa wchodzą następujące komponenty: antywirus, antyspam, antywirus sieciowy, kontrola rodzicielska (kontrola biura), zapora sieciowa firewall.
7. Dodatkowe komponenty ochrony potrzebne użytkownikowi są dodawane do licencji bazowej. Sprzedaż licencji na jeden lub kilka dodatkowych komponentów niezależnie od licencji bazowej jest niemożliwa.
8. Dla każdego typu chronionych obiektów są osobne rodzaje licencji bazowych i osobny zbiór dodatkowych komponentów.

Chronione obiekty	Wspierane SO (systemy operacyjne) i platformy	Licencja bazowa	Dodatkowe komponenty
Dr.Web Desktop Security Suite Stacje robocze Klienci serwerów terminalowych Klienci serwerów wirtualnych Klienci systemów wbudowanych	Windows 7/Vista/ XP SP2/2000	Ochrona kompleksowa	■ Centrum zarządzania ■ Kryptograf
		Antywirus	
	Mac OS X Linux	Antywirus	■ Centrum zarządzania
	MS DOS* OS/2*		
Dr.Web Server Security Suite Serwery plików Serwery aplikacji Serwery terminalowe Serwery wirtualne	Windows Novell NetWare Mac OS X Server Unix (Samba) Novell Storage Services	Antywirus	■ Centrum zarządzania
Dr.Web Mail Security Suite Użytkownicy poczty	Unix MS Exchange Lotus (Windows/Linux) Kerio (Windows/Linux)	Antywirus	■ Centrum zarządzania ■ Antyspam (oprócz Kerio) ■ SMTP proxy
Dr.Web Gateway Security Suite Użytkownicy bram internetowych	bramy internetowe Kerio bramy internetowe Unix	Antywirus	■ Centrum zarządzania
	MIMEsweeper* Qbik WinGate*		■ Antyspam
Dr.Web Mobile Security Suite Urządzenia mobilne	Windows Mobile Android	Antywirus	■ Centrum zarządzania ■ Antyspam
	Symbian OS*		■ Antyspam

*Scentralizowane zarządzanie na razie nie jest zapewnione.

Rodzaje dostawy produktów Dr.Web

Programy Dr.Web są dostarczane w postaci licencji elektronicznej lub w postaci kompletów medialnych w opakowaniu.

1. Licencja elektroniczna Dr.Web

Dostarczana jest w postaci numeru seryjnego Dr.Web:

- pocztą elektroniczną;
- na certyfikacie licencyjnym.

2. Komplet medialny Dr.Web w opakowaniu kartonowym

Kompletowanie:

- firmowe opakowanie kartonowe;
- certyfikat licencyjny;
- krótka instrukcja instalacji i rejestracji;
- płyta DVD;
- koperta firmowa na płytę;
- nalepka plombująca;
- nalepka „Chronione przez Dr.Web”;
- Nośnik USB (tylko dla produktu Dr.Web dla Mac OS X + Dr.Web Security Space Pro).

3. Rozwiązanie do modyfikacji w opakowaniu kartonowym

Rozwiązanie do modyfikacji dla jednego lub kilku produktów Dr.Web Enterprise Security Suite.

Kompletowanie:

- firmowe pudełko kartonowe Dr.WEB;
- formularz certyfikatu licencyjnego;
- płyta DVD z dystrybucją programów Dr.Web w kopercie firmowej.

4. Certyfikowany pakiet medialny

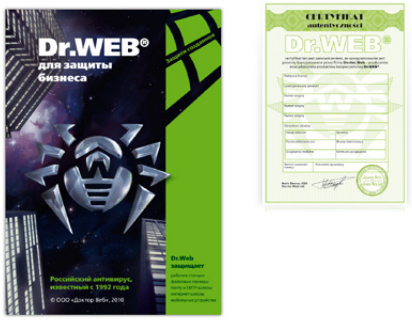
Rozwiązanie do modyfikacji dla jednego lub kilku produktów Dr.Web Enterprise Security Suite, certyfikowanych przez FSKTiE Rosji.

Kompletowanie:

- firmowe pudełko kartonowe Dr.Web;
- formularz certyfikatu licencyjnego;
- Płyta DVD z dystrybucją certyfikowanych programów Dr.Web w kopercie firmowej;
- formularz z naklejką holograficzną FSKTiE.

5. Pakiet licencyjny Dr.Web

Rozwiązanie do modyfikacji dla jednego lub kilku produktów Dr.Web Enterprise Security Suite.



Kompletowanie:

- Firmowy pakiet kartonowy Dr.Web;
- formularz certyfikatu licencyjnego.

6. Karta-zdrapka

Karta z numerem seryjnym Dr.Web, ukrytym pod paskiem do zdrapania.

7. Produkty OEM Dr.Web

Dr.Web OEM uniwersalny (licencje dla jednego użytkownika)

Dostarczany w postaci karty OEM z paskiem do zdrapania, naklejonym na ulotce OEM. Zapewnia ochronę 1 PC i 1 urządzenia mobilnego przez okres 3 miesięcy.

Skład licencji:

- Dr.Web Security Space
- Antywirus Dr.Web dla Mac OS X
- Antywirus Dr.Web dla Linux
- Dr.Web Mobile Security Suite
- Dr.Web dla Android OS
- Dr.Web dla Symbian OS
- Dr.Web dla Windows Mobile

Przedłużenie

- Aby przedłużyć okres ważności licencji OEM Dr.Web, należy nabyć licencję przedłużenia (rabat na przedłużenie jest wliczony w jej cenę).
- Można przedłużyć licencję również za pomocą ogólnodostępnych produktów Dr.Web Security Space Pro lub Antywirus Dr.Web Pro (bez rabatu na przedłużenie). W tym przypadku do okresu ważności nowej licencji zostanie dodanych 300* dni bonusowych.

* Pod warunkiem zakupu ogólnodostępnego produktu Dr.Web z licencją na ochronę 2 PC na 1 rok i kolejnej rejestracji obydwu numerów seryjnych na ochronę 1 PC.

Dostawa

Dostawa produktu Dr.Web OEM Uniwersalny do partnerów „Doctor Web" odbywa się tylko w postaci kart-zdrapek i w liczbie od 500 sztuk. Dostawa produktu w postaci kart-zdrapek lub licencji elektronicznych w liczbie od 50 do 499 sztuk następuje tylko do firm, posiadających status Autoryzowanego Centrum Serwisowego Dr.Web (bardziej szczegółowo o programie dla ACS: http://partners.drweb.com/service).

Dla dużych dostawców licencji OEM istnieje program ochrony przedłużeń licencji OEM: https://pa.drweb.com/products/oem/universal/protection/.

Dr.Web OEM serwerowy (licencje korporacyjne)

Uprawnia do korzystania z dowolnych produktów Dr.Web Enterprise Security Suite przez okres 3 miesięcy. Dostarczany w postaci pakietu medialnego.

Skład licencji:

- Centrum zarządzania Dr.Web Enterprise Security Suite
- Dr.Web Desktop Security Suite – 100 PC
- Dr.Web Server Security Suite – 10 serwerów
- Dr.Web Mail Security Suite – 100 użytkowników
- Dr.Web Gateway Security Suite – 100 użytkowników
- Dr.Web Mobile Security Suite – 100 urządzeń

Kompletowanie pakietu medialnego:

- Koperta firmowa Dr.Web
- Płyta CD z prezentacją wszystkich produktów Dr.Web
- Certyfikat licencyjny Dr.Web z numerem seryjnym na Dr.Web Enterprise Security Suite na 3 miesiące
- Ulotka „Dr.Web Enterprise Security Suite"
- Nalepka „Dr.Web OEM"

Przedłużenie

Aby przedłużyć okres ważności licencji OEM Dr.Web, należy zakupić licencję, w której cenę jest wliczony 40% rabat za przedłużenie na 1 rok.

Program bonusowy

Dla dostawców licencji serwerowych OEM jest przewidziany specjalny program bonusowy. Więcej szczegółów pod adresem: https://pa.drweb.com/products/oem/kod/bonuses.

Dr.Web Home Security Suite – produkty dla użytkowników domowych

Dr.Web Security Space

Kompleksowa ochrona PC i notebooków przed zagrożeniami internetowymi.

Zalety

- Kompleksowe rozwiązanie problemu ochrony PC. Najlepsze w branży leczenie aktywnych infekcji.
- Możliwość instalacji na zainfekowanym komputerze bez konieczności wstępnego leczenia.
- Duża szybkość skanowania dzięki wykorzystaniu możliwości systemów multiprocesorowych.
- Unikalna technologia blokady nawet nieznanych jeszcze zagrożeń (Origins Tracing).
- Pełne skanowanie archiwów o dowolnym poziomie zagnieżdżenia.
- Najlepsze wykrywanie i neutralizacja skomplikowanych wirusów.
- Efektywne filtrowanie spamu i wszystkich rodzajów niepożądanych wiadomości bez konieczności uczenia się obsługi antyspamu.
- Niezawodne skanowanie w czasie rzeczywistym wchodzącego i wychodzącego ruchu w sieci HTTP.
- Gwarantowana ochrona dzieci przed niepożądanymi treściami.
- Ochrona przed nieautoryzowanym dostępem z zewnątrz, zapobieganie wyciekom do sieci ważnych danych, blokada podejrzanych połączeń na poziomie pakietów i aplikacji (w licencjach z zaporą sieciową firewall).
- Zdalne zarządzanie programami Dr.Web na innych komputerach w granicach jednej sieci lokalnej – bez konieczności instalacji Centrum zarządzania Dr.Web.

Komponenty ochrony licencji bazowej

Skuteczne rozpoznawanie wszystkich rodzajów zagrożeń (skaner Dr.Web)

- Duża szybkość skanowania, osiągana w wyniku wielostrumieniowej obsługi danych z podziałem zadań między jądra procesora. Skaner Dr.Web uruchomi pełną moc systemów multiprocesorowych!
- Wygodny, intuicyjnie zrozumiały interfejs.
- Szybkie i niezwykle dokładne skanowanie pamięci operacyjnej, sektorów rozruchowych, dysków twardych i nośników wymiennych.
- Neutralizacja wirusów, trojanów i innych rodzajów złośliwego oprogramowania.
- Obszerne bazy do wykrywania oprogramowania szpiegowskiego, potencjalnie niebezpiecznego oraz reklamowego, narzędzi hakerskich i programów-żartów.
- Skaner konsolowy, który również zalicza się do komponentów Dr.Web, jest przeznaczony dla doświadczonych użytkowników i pozwala przeprowadzać skanowanie w trybie wiersza poleceń. Udostępnia on szerokie możliwości ustawień i jest przeznaczony, między innymi, do pracy w systemach multiprocesorowych.

Ochrona w czasie rzeczywistym (monitor plików SpIDer Guard®)

- Stały monitoring zdrowia komputera – na bieżąco przechwytuje odwołania do plików na dyskach twardych, dyskietkach, płytach CD/DVD/Blu-ray, kartach pamięci typu Flash i Smart.
- Wysoka odporność na próby przeszkadzania w funkcjonowaniu SpIDer Guard® lub zatrzymywania jego pracy ze strony złośliwego oprogramowania.

Przeciwdziałanie rootkitom (Anti-Rootkit Dr.Web Shield™)

- Niezawodna ochrona systemu przed wirusami, wykorzystującymi technologie rootkit i potrafiącymi ukrywać swoją obecność w zainfekowanym systemie.
- Neutralizacja skomplikowanych rootkitów.

Zdrowa poczta bez wirusów (monitor poczty SpIDer Mail®)...

- Kontrola w czasie rzeczywistym wirusów w poczcie zgodnie z protokołami SMTP/ POP3/ NNTP/ IMAP4.
- Kontrola szyfrowanych połączeń SSL (SMTPS/POP3S/IMAP4S).
- Kontrola nie ma wpływu na pracę użytkowanego programu pocztowego i praktycznie nie wydłuża czasu odbioru poczty.
- Indywidualne reguły obsługi każdego typu złośliwych programów – wirusów, oprogramowania potencjalnie niebezpiecznego i reklamowego, narzędzi hakerskich, płatnych dialerów, programów-żartów.
- Ochrona przed masowym rozsyłaniem wiadomości przez robaki pocztowe, dzięki analizie składu i czasu wysyłania wiadomości wychodzących, na podstawie których można wnioskować o aktywności wirusów.

... bez spamu i niechcianych wiadomości (Antyspam Dr.Web)

- Skanowanie poczty przychodzącej i wychodzącej następuje w czasie rzeczywistym.
- Praca antyspamu nie jest zależna od użytkowanego programu pocztowego i nie wydłuża czasu odbioru poczty.
- Antyspam nie wymaga konfiguracji, zaczyna działać automatycznie wraz z odbiorem pierwszej wiadomości.
- Dzięki różnym technologiom filtracji istnieje bardzo duże prawdopodobieństwo rozpoznania spamu oraz wiadomości typu phishing, pharming, scamming i bounce.
- Ochrona przed dostaniem się w botnety – dostawca nie pozbawi was dostępu do Internetu w przypadku rozsyłania spamu.
- Przefiltrowane wiadomości nie są usuwane, lecz przenoszone do specjalnego katalogu programu pocztowego, w którym, w dogodnym terminie, można sprawdzić czy nie zostały błędnie zakwalifikowane.
- Moduł analizatora spamu jest całkowicie niezależny; nie trzeba go łączyć z zewnętrznym serwerem, nie wymaga też dostępu do jakiejkolwiek bazy danych, co pozwala istotnie zmniejszyć ruch w sieci.

Ochrona poczty przechodzącej przez Microsoft Outlook

- Podłączany moduł Dr.Web dla programu Outlook sprawdza wirusy w plikach, załączonych do wiadomości pocztowych, przeprowadza kontrolę poczty przychodzącej zaszyfrowanym połączeniem SSL, filtruje spam, wykrywa i neutralizuje złośliwe oprogramowanie, korzysta z analizatora heurystycznego Dr.Web w celu dodatkowej ochrony przed nieznanymi wirusami.

Dr.Web LinkChecker — kontrola wirusów i bazy niepożądanych stron internetowych, bez instalacji Dr.Web

- Dodatki antywirusowe do kontroli stron internetowych i plików ściąganych z sieci Internet oraz do kontroli linków, zawartych we wiadomościach elektronicznych, przetwarzanych przez Mozilla Thunderbird – to wszystko bez instalacji antywirusa Dr.Web!
- Dodatki pozwalają sprawdzać strony internetowe przed ich otwarciem, ostrzegają o przechodzeniu do linków zewnętrznych w sieciach społecznościowych („W Kontaktie", Facebook, Google+) i sprawdzają te linki, wykrywają i sprawdzają zniekształcone linki, przeprowadzają kontrolę antywirusową plików przed ich pobraniem z sieci Internet, sprawdzają skrypty i ramki w linkach.

Tarcza ochronna przed zagrożeniami internetowymi (antywirus sieciowy SpIDer Gate™)

- Moduł SpIDer Gate przejrzyście skanuje w czasie rzeczywistym wchodzący przepływ HTTP, przechwytuje wszystkie połączenia HTTP, dokonuje filtracji danych, automatycznie blokuje zainfekowane strony we wszelkich przeglądarkach internetowych, skanuje pliki w archiwach (na przykład ładowane przez menedżerów i wiele innych aplikacji, wymieniających dane z serwerami sieciowymi), chroni przed zasobami internetowymi grożącymi phishingiem oraz innymi niebezpiecznymi zasobami internetowymi.
- Skanowanie szyfrowanych połączeń SSL (HTTPS).
- Blokowanie stron na podstawie bazy znanych wirusów i stron, których odwiedzania się nie zaleca.
- Możliwe jest wyłączenie kontroli przepływu wychodzącego lub wchodzącego oraz sporządzenie listy aplikacji, których przepływ HTTP będzie kontrolowany w każdym przypadku i w pełnym zakresie (czarna lista). Istnieje również możliwość wyłączenia spod kontroli ruchu sieciowego poszczególnych aplikacji (biała lista).
- Możliwe jest ustawienie priorytetów skanowania ruchu sieciowego (bilansu skanowania). Bilansowanie wpływa na podział zasobów procesora PC i szybkość pracy z Internetem.
- Praca SpIDer Gate nie jest zależna od używanej przeglądarki.
- Filtracja praktycznie nie wpływa na wydajność PC, szybkość pracy z Internetem i ilość przekazywanych danych.
- W trybie „domyślnym" nie jest wymagana żadna konfiguracja: Dr.Web SpIDer Gate zaczyna skanowanie od razu po instalacji w systemie.

Kontrola przeglądania zasobów Internetu (Kontrola rodzicielska Dr.Web)

- Ochrona dzieci przed odwiedzaniem niepożądanych stron.
- Blokowanie stron internetowych według 10 grup tematycznych (broń, narkotyki, gry, pornografia i inne).
- Zakaz używania pamięci przenośnych (dysków typu Flash, urządzeń USB), urządzeń sieciowych oraz oddzielnych plików i katalogów – dodatkowa możliwość zabezpieczenia informacji przed usunięciem lub wykradzeniem przez przestępców internetowych.

Ochrona przed atakami sieciowymi (zapora sieciowa Dr.Web)

- Ochrona przed nieautoryzowanym dostępem z zewnątrz, zapobieganie wyciekom ważnych danych przez sieć, blokada podejrzanych połączeń na poziomie pakietów i aplikacji.
- Kontrola połączeń na poziomie aplikacji pozwala na kontrolowanie dostępu konkretnych programów i procesów do zasobów sieciowych oraz na rejestrowanie informacji o próbach dostępu w dzienniku aplikacji.
- Filtracja na poziomie pakietów pozwala na kontrolowanie dostępu do sieci internetowej niezależnie od programów inicjujących podłączenie. Dziennik filtracji pakietów przechowuje informacje o pakietach przekazanych przez interfejsy sieciowe.
- Istnienie tak zwanego „trybu gry", przy włączeniu którego okno z żądaniem utworzenia reguły pojawia się na wierzchu każdej aplikacji uruchomionej w trybie pełnoekranowym.
- Monitoring aplikacji, wykorzystujących sieć w czasie rzeczywistym, z możliwością przymusowego zakończenia połączenia.

Zdalne zarządzanie

- Funkcja „Sieć antywirusowa" pozwala zdalnie zarządzać antywirusami Dr.Web, zainstalowanymi na komputerach w obrębie jednej sieci lokalnej.
- Do zdalnego zarządzania nie jest wymagana instalacja Centrum zarządzania Dr.Web.
- Podłączenie jest możliwe z dowolnego komputera do innego dowolnego komputera z tej samej sieci lokalnej.

- Możliwości zarządzania obejmują: uzyskanie statystyki i rejestru zdarzeń z oddalonej stacji, odczytywanie i zmienianie na niej ustawień modułów, ich uruchamianie i zatrzymywanie. Dostępna jest również rejestracja numeru seryjnego i zamiana pliku klucza na oddalonej stacji.
- Do zdalnego dostępu wymagane jest włączenie zezwolenia na taki dostęp w oddalonej stacji.

Dodatkowe komponenty

Kryptograf Atlansys Bastion Pro*

- Szyfrowanie informacji w specjalnych pakietach plików, do których nie można uzyskać dostępu, nie znając hasła.
- Wsparcie pracy większości znanych algorytmów szyfrowania.
- Podłączony tajny dysk jest dostępny jako zwykły logiczny dysk systemowy.
- Bezpieczna praca z zaszyfrowanymi informacjami zarówno na komputerze wolno stojącym, jak i przy podłączaniu go do sieci.
- Usuwanie zbędnych plików bez możliwości odtworzenia zawartych w nich informacji.
- Do pracy nie jest wymagana specjalistyczna wiedza. Szczegółowy system podpowiedzi pozwala na szybkie przyswojenie różnych możliwości systemu.

* Tylko w licencji z kryptografem. Atlansys Bastion Pro opracowała firma „Systemy programowe Atlansys" www.atlansys.ru.

Wersje licencji

- Dr.Web Security Space
- Dr.Web Security Space + Kryptograf

Wspierane systemy operacyjne

- Windows 7/Vista/XP SP2/2000 SP4 + Rollup 1 (systemy 32- i 64-bitowe).
- Kryptograf Atlansys Bastion Pro działa na komputerach sterowanych przez Windows 7/Vista/XP (systemy 32- i 64-bitowe).

Wolne miejsce na dysku twardym

- 450 MB*
- Dodatkowo do instalacji zapory sieciowej potrzeba ~ 11 MB.
- Wolne miejsce na dysku twardym na kryptograf: ~ 50 MB.

* Pliki tymczasowe, tworzone w trakcie instalacji, będą wymagały dodatkowego miejsca.

Przydatne linki

Opis: http://products.drweb.com/win/security_space

Antywirus Dr.Web dla Windows

Minimum niezbędnej ochrony PC i notebooków przed wirusami i programami szpiegowskimi

Zalety

- Najlepsze w branży leczenie aktywnych infekcji.
- Możliwość instalacji na zainfekowanym komputerze bez konieczności wstępnego leczenia.
- Duża szybkość skanowania dzięki wykorzystaniu możliwości systemów multiprocesorowych.
- Unikalna technologia blokady nawet nieznanych jeszcze zagrożeń (Origins Tracing).
- Pełne skanowanie archiwów o dowolnym poziomie zagnieżdżenia.
- Najlepsze wykrywanie i neutralizacja skomplikowanych wirusów.
- Ochrona przed nieautoryzowanym dostępem z zewnątrz, zapobieganie wyciekom ważnych danych przez sieć, blokada podejrzanych połączeń na poziomie pakietów i aplikacji (w licencjach z zaporą sieciową firewall).

Komponenty ochrony licencji bazowej

Skuteczne rozpoznawanie wszystkich rodzajów zagrożeń (skaner Dr.Web)

- Duża szybkość skanowania, osiągana w wyniku wielostrumieniowej obsługi danych z podziałem zadań między jądra procesora. Skaner Dr.Web uruchomi pełną moc systemów multiprocesorowych!
- Wygodny, intuicyjnie zrozumiały interfejs.
- Szybkie i niezwykle dokładne skanowanie pamięci operacyjnej, sektorów rozruchowych, dysków twardych i nośników wymiennych.
- Neutralizacja wirusów, trojanów i innych rodzajów złośliwego oprogramowania.
- Obszerne bazy do wykrywania oprogramowania szpiegowskiego, potencjalnie niebezpiecznego oraz reklamowego, narzędzi hakerskich i programów-żartów.
- Skaner konsolowy, który również zalicza się do komponentów Dr.Web, jest przeznaczony dla doświadczonych użytkowników i pozwala przeprowadzać skanowanie w trybie wiersza poleceń. Udostępnia on szerokie możliwości ustawień i jest przeznaczony, między innymi, do pracy w systemach multiprocesorowych.

Ochrona w czasie rzeczywistym (monitor plików SpIDer Guard®)

- Stały monitoring zdrowia komputera – na bieżąco przechwytuje odwołania do plików na dyskach twardych, dyskietkach, płytach CD/DVD/Blu-ray, kartach pamięci typu Flash i Smart.
- Wysoka odporność na próby przeszkadzania w funkcjonowaniu SpIDer Guard® lub zatrzymywania jego pracy ze strony złośliwego oprogramowania.

Przeciwdziałanie rootkitom (Anti–Rootkit Dr.WEB Shield™)

- Niezawodna ochrona systemu przed wirusami, wykorzystującymi technologie rootkit i potrafiącymi ukrywać swoją obecność w zainfekowanym systemie.
- Neutralizacja skomplikowanych rootkitów.

Zdrowa poczta bez wirusów (monitor poczty SpIDer Mail®)

- Kontrola w czasie rzeczywistym wirusów w poczcie, zgodnie z protokołami SMTP/POP3/NNTP/IMAP4.
- Kontrola szyfrowanych połączeń SSL (SMTPS/POP3S/IMAP4S).
- Kontrola nie ma wpływu na pracę użytkowanego programu pocztowego i praktycznie nie wydłuża czasu odbioru poczty.

- Indywidualne reguły obsługi każdego typu złośliwych programów – wirusów, oprogramowania potencjalnie niebezpiecznego i reklamowego, narzędzi hakerskich, płatnych dialerów, programów-żartów.
- Ochrona przed masowym rozsyłaniem wiadomości przez robaki pocztowe, dzięki analizie składu i czasu wysyłki wiadomości wychodzących, na podstawie których można wnioskować o aktywności wirusów.

Ochrona poczty przechodzącej przez Microsoft Outlook

- Podłączany moduł Dr.Web dla programu Outlook sprawdza wirusy w plikach, załączonych do wiadomości pocztowych, przeprowadza kontrolę poczty przychodzącej zaszyfrowanym połączeniem SSL, filtruje spam, wykrywa i neutralizuje złośliwe oprogramowanie, korzysta z analizatora heurystycznego Dr.Web w celu dodatkowej ochrony przed nieznanymi wirusami.

Dr.Web LinkChecker – kontrola wirusów i bazy niepożądanych stron internetowych, bez instalacji Dr.Web

- Dodatki antywirusowe do kontroli stron internetowych i plików ściąganych z sieci Internet oraz do kontroli linków, zawartych we wiadomościach elektronicznych, przetwarzanych przez Mozilla Thunderbird – i to wszystko bez instalacji antywirusa Dr.Web!
- Dodatki pozwalają sprawdzać strony internetowe przed ich otwarciem, ostrzegają o przechodzeniu do linków zewnętrznych w sieciach społecznościowych („W Kontaktie", Facebook, Google+) i sprawdzają te linki, wykrywają i sprawdzają zniekształcone linki, przeprowadzają kontrolę antywirusową plików przed ich pobraniem z sieci Internet, sprawdzają skrypty i ramki w linkach.

Ochrona przed atakami sieciowymi (zapora sieciowa Dr.Web)

- Ochrona przed nieautoryzowanym dostępem z zewnątrz, zapobieganie wyciekom ważnych danych przez sieć, blokada podejrzanych połączeń na poziomie pakietów i aplikacji.
- Kontrola połączeń na poziomie aplikacji pozwala na kontrolowanie dostępu konkretnych programów i procesów do zasobów sieciowych oraz na rejestrowanie informacji o próbach dostępu w dzienniku aplikacji.
- Filtracja na poziomie pakietów pozwala na kontrolowanie dostępu do sieci internetowej niezależnie od programów inicjujących podłączenie. Dziennik filtracji pakietów przechowuje informacje o pakietach przekazanych przez interfejsy sieciowe.
- Istnienie tak zwanego „trybu gry", przy włączeniu którego okno z żądaniem utworzenia reguły pojawia się na wierzchu każdej aplikacji uruchomionej w trybie pełnoekranowym.
- Monitoring aplikacji, wykorzystujących sieć w czasie rzeczywistym, z możliwością przymusowego zakończenia połączenia.

Zdalne zarządzanie

- Funkcja „Sieć antywirusowa" pozwala zdalnie zarządzać antywirusami Dr.Web, zainstalowanymi na komputerach w obrębie jednej sieci lokalnej.
- Do zdalnego zarządzania nie jest wymagana instalacja Centrum zarządzania Dr.Web.
- Podłączenie jest możliwe z dowolnego komputera do innego dowolnego komputera z tej samej sieci lokalnej.
- Możliwości zarządzania obejmują: uzyskanie statystyki i rejestru zdarzeń z oddalonej stacji, odczytywanie i zmienianie na niej ustawień modułów, ich uruchamianie i zatrzymywanie. Dostępna jest również rejestracja numeru seryjnego i zamiana pliku klucza na oddalonej stacji.
- Do zdalnego dostępu wymagane jest włączenie zezwolenia na taki dostęp w oddalonej stacji.

Dodatkowe komponenty

Kryptograf Atlansys Bastion Pro*

- Szyfrowanie informacji w specjalnych pakietach plików, do których nie można uzyskać dostępu, nie znając hasła.
- Wsparcie pracy większości znanych algorytmów szyfrowania.
- Podłączony tajny dysk jest dostępny jako zwykły logiczny dysk systemowy.
- Bezpieczna praca z zaszyfrowanymi informacjami zarówno na komputerze wolno stojącym, jak i przy podłączaniu go do sieci.
- Usuwanie zbędnych plików bez możliwości odtworzenia zawartych w nich informacji.
- Do pracy nie jest wymagana specjalistyczna wiedza. Szczegółowy system podpowiedzi pozwala na szybkie przyswojenie różnych możliwości systemu.

* Tylko w licencji z kryptografem. Atlansys Bastion Pro opracowała firma „Systemy programowe Atlansys ”www.atlansys.ru.

Wersje licencji

- Antywirus
- Antywirus + Kryptograf

Wspierane systemy operacyjne

- Windows 7/Vista/XP SP2/2000 SP4 + Rollup 1 (systemy 32- i 64-bitowe).
- Kryptograf Atlansys Bastion Pro działa na komputerach sterowanych przez Windows 7/Vista/XP (systemy 32- i 64-bitowe).

Wolne miejsce na dysku twardym

- 350 MB*
- Dodatkowo do instalacji zapory potrzeba ~ 11 MB.
- Wolne miejsce na dysku twardym na kryptograf: ~ 50 MB.

* Pliki tymczasowe, tworzone w trakcie instalacji, będą wymagały dodatkowego miejsca.

Przydatne linki

Opis: http://products.drweb.com/win

Antywirus Dr.Web dla Mac OS X

Minimum niezbędnej ochrony przed wirusami i innymi złośliwymi programami, napisanymi w celu infekowania nie tylko Mac OS X, ale i innych systemów operacyjnych.

Funkcje kluczowe

- Skanowanie obiektów autouruchamiania, wymiennych nośników informacji, dysków sieciowych i logicznych, formatów pocztowych, plików i katalogów, włącznie z tymi zapakowanymi i znajdującymi się w archiwach.
- Szybkie skanowanie pełne i fragmentaryczne.
- Skanowanie antywirusowe ręczne, automatyczne lub na podstawie wcześniej stworzonego harmonogramu.
- Ochrona regulacji monitora SpIDerGuard® za pomocą hasła chroniącego przed nieautoryzowanymi zmianami.
- Stosowanie czynności wobec zainfekowanych i podejrzanych obiektów oraz obiektów innego rodzaju, włącznie z leczeniem, przeniesieniem do kwarantanny i usunięciem, w tym również wtedy, gdy wybrana wcześniej czynność okazała się niemożliwą do wykonania.
- Wyłączenie ze skanowania ścieżek i plików na życzenie użytkownika.
- Wykrywanie i usuwanie wirusów ukrytych w formatach nieznanych programów do pakowania.
- Rejestrowanie czasu zdarzenia, obiektu skanowania i rodzaju podjętego w związku z nim działania.
- Instalacja aktualizacji: automatyczna (zgodnie z harmonogramem) lub na żądanie.
- Automatyczne powiadomienie (w tym z użyciem powiadomień dźwiękowych) o zdarzeniach wirusowych.
- Izolacja zainfekowanych plików w kwarantannie z możliwością zaprogramowania czasu przechowywania obiektów w kwarantannie i jej maksymalnego rozmiaru.
- Leczenie, odzyskiwanie lub usuwanie obiektów przeniesionych do kwarantanny. Prowadzenie szczegółowego raportu pracy.
- Dostępność modułów w formie narzędzi wiersza polecenia, z możliwością ich integracji z Apple Scripts używanymi do obsługi systemu.

Zalety

- Komfortowe Centrum zarządzania.
- Duża szybkość skanowania.
- Możliwość tworzenia własnych profili skanowania.
- Niezawodna ochrona w czasie rzeczywistym.
- Minimalne obciążenie chronionego systemu.
- Niewielki ruch sieciowy przy aktualizacjach.
- Różnorodne konfiguracje.
- Łatwość zarządzania.
- Nowoczesny i wygodny interfejs.

Wymagania systemowe

- Mac OS X 10.4 lub w wyższej wersji (systemy 32- i 64-bitowe).
- Procesor Intel.
- 128 MB pamięci operacyjnej.
- 120 MB wolnego miejsca na dysku twardym.
- Dostęp do sieci internetowej: w celu dokonania rejestracji i uzyskania aktualizacji.

Przydatne linki

Opis: http://products.drweb.com/mac

Antywirus Dr.Web dla Linux

Minimum niezbędnej ochrony przed wirusami

Funkcje kluczowe

- Wykrywanie i neutralizacja wirusów oraz innych obiektów złośliwych na dyskach twardych i nośnikach wymiennych.
- Identyfikacja wirusów w archiwach o dowolnym poziomie zagnieżdżenia oraz w obiektach spakowanych.
- Skanowanie plików, skompresowanych przez programy do pakowania, również nieznane, za pomocą technologii FLY-CODE™.
- Ochrona przed nieznanymi zagrożeniami za pomocą technologii bezsygnaturowego wykrywania OriginsTracing™ i inteligentnego analizatora heurystycznego Dr.Web.
- Skanowanie szybkie, pełne, fragmentaryczne lub inne określone przez użytkownika.
- Stały monitoring zdrowia komputera – przechwytuje na bieżąco odwołania do plików na dyskach twardych, dyskietkach, napędach CD/DVD/Blu-ray, kartach pamięci typu Flash i Smart.
- Ochrona własnych komponentów przed próbami zakłócenia pracy antywirusa przez złośliwe oprogramowanie.
- Izolacja zainfekowanych obiektów w kwarantannie z możliwością ich przywrócenia; funkcja ograniczenia rozmiaru kwarantanny.
- Gromadzenie wszystkich danych statystycznych dotyczących pracy antywirusa.
- Automatyczne aktualizacje – zaplanowane i na żądanie.

Zalety

- Komfortowe Centrum zarządzania.
- Możliwość skanowania w czasie rzeczywistym.
- Konfiguracja skanowania ustalona przez użytkownika.
- Kwarantanna na żądanie.
- Automatyczne aktualizacje.
- Nowoczesny interfejs.

Wymagania systemowe

- Platforma: pełne wsparcie systemu poleceń procesora architektury x86 w trybie 32- i 64-bitowym.
- Co najmniej 154 MB wolnego miejsca na dysku + 70 MB dla każdego użytkownika.
- System operacyjny: dystrybucje GNU/Linux posiadające jądro w wersji 2.6.x.
- Dostęp do sieci internetowej: w celu dokonania rejestracji i uzyskania aktualizacji.

Przydatne linki

Opis: http://products.drweb.com/linux

Skanery konsolowe Dr.Web

Ochrona antywirusowa z rozszerzonymi możliwościami jej automatyzacji dla doświadczonych użytkowników

Skanery konsolowe Dr.Web bez graficznego interfejsu wykorzystują ogólną bazę wirusów i moduł wyszukiwania Dr.Web; przeznaczone są do pracy w systemach operacyjnych MSDOS, OS/2 i Windows. Do zarządzania ochroną antywirusową niezbędne jest doświadczenie w pracy z panelem poleceń.

Zalety

- Minimalne wymagania systemowe – skanery bardzo dobrze pracują nawet w systemach wbudowanych i są w stanie niezawodnie chronić komputery poprzednich generacji o małej mocy.
- Komfort w skanowaniu – administrator może wybrać skanowanie „ręczne" lub zaplanowane.
- Leczenie zainfekowanych stacji roboczych i serwerów, w tym niedostępnych w sieci.
- Bardzo duża odporność na wirusy i możliwość instalacji na zainfekowanym komputerze.
- Automatyzacja codziennych prac z wykorzystaniem ogromnych możliwości panela poleceń.
- Gwarancja usunięcia wirusów nieznanych programowi Dr.Web lub wirusów nieznanego formatu, znajdujących się w archiwach.
- Uruchamianie z dowolnego zewnętrznego nośnika (płyty CD lub nośnika USB).

Przydatne linki

Opis: http://products.drweb.com/console/

„Dr.Web Uniwersalny" (dla klientów ACS)

Kompleksowa ochrona PC i notebooków dla klientów Autoryzowanych Centrów Serwisowych Dr.WEB.

Licencje elektroniczne produktu „Dr.Web Uniwersalny" są dostarczane tylko przez Autoryzowane Centra Serwisowe Dr.Web.

„Dr.Web Uniwersalny" zapewnia ochronę 1 PC i 1 urządzenia mobilnego przez 1 rok.

Skład licencji:

- Dr.Web Security Space
- Antywirus Dr.Web dla Mac OS X
- Antywirus Dr.Web dla Linux
- Dr.Web Mobile Security Suite
- Dr.Web dla Android OS
- Dr.Web dla Symbian OS
- Dr.Web dla Windows Mobile

Bardziej szczegółowo o autoryzowanych centrach Dr.Web –
http://partners.drweb.com/service/

Dr.Web Enterprise Security Suite. Produkty dla przedsiębiorstw

Dr.Web Enterprise Security Suite – – to zestaw produktów Dr.Web, który zawiera elementy ochrony wszystkich węzłów sieci korporacyjnej i wspólne centrum zarządzania dla większości z nich.

Produkty podzielono na 5 grup, zależnie od rodzaju obiektów, które chronią. Przy określonych wymaganiach klienta znacznie ułatwia to poszukiwanie potrzebnego produktu.

Produkt	Produkty programowe
Dr.Web® Desktop Security Suite Ochrona stacji roboczych, klientów serwerów terminalowych, klientów serwerów wirtualnych i klientów systemów wbudowanych	Dr.Web dla Windows
	Dr.Web dla Linux
	Dr.Web dla Mac OS X
	Dr.Web dla MS DOS*
	Dr.Web dla OS/2*
Dr.Web® Server Security Suite Ochrona serwerów plików i serwerów aplikacji (w tym wirtualnych i terminalowych)	Dr.Web dla serwerów Windows
	Dr.Web dla serwerów Unix
	Dr.Web dla serwerów Novell NetWare
	Dr.Web dla serwerów Mac OS X Server
	Dr.Web dla Novell Storage Services
Dr.Web® Mail Security Suite Ochrona poczty	Dr.Web dla serwerów pocztowych i bram internetowych Unix
	Dr.Web dla MS Exchange
	Dr.Web dla IBM Lotus Domino dla Windows
	Dr.Web dla IBM Lotus Domino dla Linux
	Dr.Web dla serwerów pocztowych Kerio dla Windows
	Dr.Web dla serwerów pocztowych Kerio dla Linux
	Dr.Web dla serwerów pocztowych Kerio dla Mac
Dr.Web® Gateway Security Suite Ochrona bram internetowych	Dr.Web dla bram internetowych Unix
	Dr.Web dla bram internetowych Kerio
	Dr.Web dla MIMEsweeper*
	Dr.Web dla Qbik WinGate*
Dr.Web® Mobile Security Suite Ochrona urządzeń mobilnych	Dr.Web dla Windows Mobile
	Dr.Web dla Symbian OS*
	Dr.Web dla Android

* Scentralizowane zarządzanie na razie nie jest zapewnione.

Algorytm wyboru potrzebnego produktu

1. Co muszą Państwo chronić?	2. W jakim systemie operacyjnym/ na jakiej platformie działają chronione urządzenia?*	3. Czy potrzebują Państwo tylko antywirusa, czy kompleksowej ochrony?	4. Czy potrzebują Państwo kryptograficznej ochrony informacji?	5. Ile obiektów trzeba chronić?	6.Na jaki okres potrzebna jest licencja?	7. Czy wymagana licencja jest pierwszym zakupem, przedłużeniem, dodatkowym zakupem, dodatkowym zakupem z przedłużeniem? czy klientowi przysługuje rabat?
Określamy produkt	Określamy system operacyjny/ platformę	Określamy licencję bazową	Określamy dodatkowe komponenty	Określamy liczbę licencji	Określamy okres obowiązywania licencji	Określamy typ licencji i ewentualne rabaty
Stacje robocze (Dr.Web Desktop Security Suite)	■ Windows 7/Vista/ XP/2000 SP 4 + Rollup 1	■ Ochrona kompleksowa ■ Antywirus	■ Centrum zarządzania ■ Kryptograf	1....	12,24 lub 36 miesięcy	
	■ Mac OS X ■ Linux MS DOS OS/2	■ Antywirus	■ Centrum zarządzania			
Serwery plików (Dr.Web Server Security Suite)	■ Windows ■ Novell ■ NetWare ■ Mac OS X Server ■ Unix ■ Novell Storage Services	■ Antywirus	■ Centrum zarządzania	1...		
Ruch sieciowy w poczcie (Dr.Web Mail Security Suite)	■ Unix ■ MS Exchange ■ Lotus Domino ■ Kerio	■ Antywirus	■ Antyspam ■ SMTP Proxy ■ Centrum zarządzania	■ Nieograniczona liczba użytkowników ■ Serwery – z liczbą chronionych użytkowników nie większą niż 3000		
Ruch sieciowy w Internecie (Dr.Web Gateway Security Suite)	■ Bramy internetowe Kerio ■ Bramy internetowe Unix	■ Antywirus	■ Centrum zarządzania	■ Nieograniczona liczba użytkowników		
	■ Qbik WinGate ■ MIMEsweeper		■ Antyspam	■ Serwery – z liczbą chronionych użytkowników nie większą niż 3000		
Urządzenia mobilne (Dr. Web Mobile Security Suite)	■ Windows Mobile ■ Android	■ Antywirus	■ Antyspam ■ Centrum zarządzania	■ Nieograniczona liczba urządzeń mobilnych		
	■ Symbian OS		■ Antyspam			
Teraz mają Państwo wszystkie informacje, potrzebne do obliczenia kosztu licencji.						

* Ten krok jest ważny tylko przy wyborze ochrony dla stacji roboczych, ponieważ od używanego systemu operacyjnego zależy zbiór dostępnych dodatkowych komponentów (Zob. „Licencjonowanie produktów").

Centrum zarządzania Dr.Web

Scentralizowane zarządzanie ochroną wszystkich węzłów sieci korporacyjnej

Funkcje kluczowe

Scentralizowane zarządzanie wszystkimi komponentami ochrony, śledzenie stanu wszystkich chronionych węzłów, konfiguracja automatycznej reakcji na incydenty wirusowe.

Zalety

- Niskonakładowe zarządzanie systemem ochrony sieci korporacyjnej z dowolnego miejsca na ziemi, z jednego stanowiska pracy (poprzez administratora sieci), gdziekolwiek by się ono nie znajdowało, nawet poza siecią korporacyjną.
- Minimalny łączny koszt w porównaniu z konkurencyjnymi programami dzięki możliwości rozwijania sieci na serwerach Windows i UNIX, łatwej instalacji i pewności ochrony.
- System ochrony można rozwijać praktycznie w każdej sieci korporacyjnej, niezależnie od jej rozmiaru i właściwości – łącznej liczby pracowników i oddziałów, topologii, obecności lub braku serwera Active Directory.
- Możliwość rozwijania agentów na stacjach roboczych w sposób wygodny dla administratora – poprzez polityki Active Directory, skrypty startowe, mechanizmy zdalnej instalacji. Instalacja jest możliwa nawet wtedy, gdy węzeł sieci jest zamknięty i niedostępny dla serwera antywirusowego.
- Możliwość realizacji indywidualnej polityki bezpieczeństwa dla konkretnego przedsiębiorstwa i poszczególnych grup pracowników.
- Automatyzacja pracy dzięki integracji z systemem Windows NAP.
- Wyjątkowa skalowalność dla sieci o dowolnym rozmiarze i złożoności. Skalowanie możliwe jest dzięki wykorzystaniu hierarchii współdziałających serwerów antywirusowych Centrum zarządzania i oddzielnego serwera SQL dla przechowywania danych oraz dzięki istnieniu kompleksowej struktury współdziałania między nimi a chronionymi węzłami sieci.
- Wsparcie dla kilku protokołów sieciowych do wymiany danych między chronionymi komputerami a serwerem antywirusowym: TCP/IP (włącznie z IPv6), IPX/SPX i NetBIOS, dzięki czemu można używać go w najróżniejszych sieciach.
- Bezpieczny przekaz danych między komponentami systemu dzięki możliwości szyfrowania.
- Minimalny ruch w sieci. Kompresję danych między klientem a serwerem zapewnia specjalnie opracowany protokół wymiany informacji w sieciach, zbudowanych na bazie protokołów TCP/IP, IPX/SPX lub NetBIOS.
- Przejrzystość pracy – dziennik audytowy rejestrujący czynności administratorów pozwala na śledzenie wszystkich kroków dotyczących instalacji i konfiguracji systemu. Wszystkie jego komponenty mogą tworzyć pliki z raportami o regulowanym poziomie uszczegółowienia.
- Wygodny system powiadamiania administratora o problemach, powstających w sieci antywirusowej.
- Możliwość wyznaczania odrębnych administratorów dla różnych grup, dzięki czemu można korzystać z Centrum zarządzania zarówno w firmach o podwyższonych wymaganiach bezpieczeństwa, jak i w organizacjach wielooddziałowych.
- Możliwości konfigurowania polityk bezpieczeństwa dla dowolnego rodzaju użytkowników, łącznie z „mobilnymi”, i dla dowolnych stacji – nawet nieobecnych w danym momencie w sieci – zapewniają aktualność ochrony w dowolnym czasie.
- Gwarancja braku możliwości samodzielnej zmiany regulacji ochrony przez użytkowników.
- Możliwość ochrony sieci nieposiadających dostępu do Internetu.
- Możliwość korzystania z większości istniejących baz danych, zarówno wewnętrznych, jak i zewnętrznych. Przy tym jako te ostatnie mogą występować Oracle, PostgreSQL, MicrosoftSQLServer lub Microsoft SQL Server Compact Edition, dowolny system zarządzania bazami danych ze wsparciem SQL-92 przez ODBC.

- Możliwość samodzielnego napisania programów obsługi zdarzeń w jakimkolwiek języku skryptowym, co daje bezpośredni dostęp do wewnętrznych interfejsów Centrum zarządzania.
- Możliwość cofnięcia aktualizacji – nawet wtedy, gdy proces aktualizacji spowodował błąd, węzeł sieci nie pozostanie bez ochrony.
- Otwartość – za pomocą tego zestawu administrator systemowy może instalować i synchronizować dodatkowe produkty postronnych producentów, co pozwala zmniejszyć koszty budowania systemów bezpieczeństwa informacyjnego.
- Przejrzystość systemu kontroli stanu ochrony, nieprześcignione pod względem skuteczności i komfortu wyszukiwanie stacji sieci.
- Możliwości wyboru listy aktualizowanych komponentów produktu i kontrola przejścia na nowe wersje pozwalają administratorom instalować tylko niezbędne i sprawdzone w ich sieci aktualizacje.

Dr.Web Desktop Security Suite

Ochrona stacji roboczych, klientów serwerów terminalowych, klientów serwerów wirtualnych i klientów systemów wbudowanych.

- Dr.Web dla Windows – certyfikowany przez FSKTiE Rosji
- Dr.Web dla Linux – certyfikowany przez FSKTiE Rosji
- Dr.Web dla Mac OS X
- Skanery konsolowe Dr.Web dla Windows, MS DOS, OS/2

Wspierane systemy operacyjne

Dr.Web dla Windows	Dr.Web dla Linux	Dr.Web dla Mac OS X	Skanery konsolowe Dr.Web
Windows 7/Vista/XP/2000 (systemy 32- i 64-bitowe)	Dystrybucje z jądrem Linux w wersji 2.6.x (systemy 32- i 64-bitowe)	Mac OS X 10.4 i w wyższej wersji	Windows, MS DOS, OS/2

Licencjonowanie Dr.Web Desktop Security Suite

Rodzaje ochrony

Ze względu na liczbę chronionych stacji roboczych, klientów podłączonych do serwera terminalowego lub klientów systemów wbudowanych.

Produkty programowe Dr.Web Desktop Security Suite można nabyć oddzielnie lub w zestawie Dr.Web Enterprise Security Suite. W ostatnim przypadku udzielana jest dodatkowo licencja na Centrum zarządzania Dr.Web Enterprise Security Suite (z wyłączeniem skanerów konsolowych Dr.Web) i na kryptograf (tylko dla Dr.Web dla Windows).

Wersje licencji

	Windows 7/Vista/XP/2000 SP 4 + Rollup 1	Windows 7/Vista/XP/2000	Linux	Mac OS X	MS DOS, OS/2
Licencja bazowa	Ochrona kompleksowa	Antywirus Windows 7/Vista/XP/2000SP4 + Rollup1			
Komponenty ochrony licencji bazowej	■ Antywirus ■ Antyszpieg ■ Anty-rootkit ■ Antyspam ■ Antywirus sieciowy ■ Kontrola biura ■ Zapora	■ Antywirus ■ Antyszpieg ■ Anty-rootkit ■ Zapora	■ Antywirus ■ Antyszpieg	■ Antywirus ■ Antyszpieg ■ Anty-rootkit	■ Antywirus ■ Antyszpieg ■ Anty-rootkit
Dodatkowe komponenty					
Centrum zarządzania	+	+	+	+	–
Kryptograf	+	+	–	–	–

Produkty grupy Dr.Web Desktop Security Suite (z wyłączeniem skanerów konsolowych) dostępne są również w zestawach ekonomicznych Dr.Web dla małych i średnich przedsiębiorstw.

Informacje o produktach programowych Dr.Web dla Windows, Mac OS X, Linux i skanerach konsolowych znajdują się w rozdziale „Dr.Web Home Security Suite. Produkty dla domu". Informacje o produkcie Dr.Web Security Space odpowiadają licencji „Ochrona kompleksowa".

Dr.Web Server Security Suite

Ochrona serwerów plików i serwerów aplikacji (w tym serwerów terminalowych)

- Dr.Web dla serwerów Windows – certyfikowany przez FSKTiE Rosji
- Dr.Web dla Mac OS X Server
- Dr.Web dla serwerów Novell NetWare
- Dr.Web dla serwerów Unix (Samba) – certyfikowany przez FSKTiE Rosji
- Dr.Web dla Novell Storage Services

Wspierane systemy operacyjne

Dr.Web dla serwerów Windows	Dr.Web dla serwerów Unix	Dr.Web dla serwerów Novell NetWare	Dr.Web dla Mac OS X Server	Dr.Web dla Novell Storage Services
Windows Server 2000* / 2003 (x32 i x64*) / 2008 / 2012 (x64)	■ Linux z jądrem w wersji 2.4.x i wyższej. ■ Free BSD w wersji 6.x i wyższej dla platformy Intel x86 ■ Solaris w wersji 10(dla platformy Intel x86	Novell NetWare w wersji 3.12-6.5	Mac OS X Se-rver w wersji 10.4 i wyższej.	SUSE Linux Enter-prise Server 10 SP3

* Tylko dla wersji 7.0.

Produkty programowe Dr.Web Server Security Suite można nabyć oddzielnie lub w zestawie Dr.Web Enterprise Security Suite. W ostatnim przypadku udzielana jest dodatkowo licencja na Centrum zarządzania Dr.Web Enterprise Security Suite.

	Dr.Web dla serwerów Windows	Dr.Web dla serwerów Novell NetWare	Dr.Web dla serwerów Unix	Dr.Web dla Mac OS X Server	Dr.Web dla Novell Storage Services
Licencja bazowa	Antywirus				
Dodatkowe komponenty					
Centrum zarządzania	+	+	+	+	+

Wszystkie produkty Dr.Web Server Security Suite dostępne są również w zestawach ekonomicznych Dr.Web dla małych i średnich przedsiębiorstw.

Dr.Web dla serwerów Windows

Ochrona antywirusowa serwerów plików i serwerów terminalowych sterowanych przez Windows, łącznie z serwerami aplikacji

Zalety

- Możliwość wykorzystania w organizacjach, wymagających podwyższonego poziomu bezpieczeństwa – produkt całkowicie spełnia wymagania prawa rosyjskiego i posiada certyfikaty zgodności Federalnej Służby Kontroli Technicznej i Eksportowej oraz Federalnej Służby Bezpieczeństwa.
- Duża efektywność i stabilność pracy.

- Duża prędkość skanowania przy minimalnym obciążeniu systemu operacyjnego, dzięki czemu Dr.Web może doskonale funkcjonować na serwerach o praktycznie dowolnej konfiguracji.
- Praca antywirusa bez zakłóceń w trybie automatycznym.
- Elastyczny rozkład obciążenia systemu plików serwera dzięki unikalnej technologii opóźnionego skanowania plików otwartych „do odczytu".
- Elastyczny, zorientowany na klienta system konfiguracji – wybór obiektów do skanowania, czynności z wykrytymi wirusami lub podejrzanych plików.
- Prosta instalacja i administracja.
- Pełnowartościowa ochrona od razu po zainstalowaniu (z domyślnymi konfiguracjami).
- Przejrzystość – szczegółowe pliki raportu o niezbędnym administratorowi stopniu uszczegółowienia.

Funkcje kluczowe

- Skanowanie sektorów serwera zgodnie z ustalonym wcześniej planem lub na żądanie administratora.
- Skanowanie „na bieżąco" – bezpośrednio podczas zapisywania lub otwierania plików na serwerze ze stacji roboczych.
- Skanowanie wielowątkowe.
- Automatyczne odłączanie od serwera stacji będącej źródłem zagrożenia wirusowego.
- Błyskawiczne informowanie administratora oraz innych użytkowników i grup o incydentach wirusowych – pocztą elektroniczną lub poprzez wysłanie powiadomień na telefon komórkowy lub pager.
- Izolacja zainfekowanych plików w kwarantannie.
- Leczenie, odzyskiwanie i/lub usuwanie plików z kwarantanny.
- Prowadzenie dziennika czynności antywirusa.
- Automatyczne aktualizacje baz wirusów.
- Neutralizacja zagrożeń nawet podczas instalacji.
- Inteligentna optymalizacja uwzględnia dostępne zasoby systemu.
- Technologia skanowania wielowątkowego i optymalizacja wydajności pozwalają uzyskać maksymalnie dużą szybkość skanowania.
- System powiadomień nie przeszkadza użytkownikowi poprzez wyskakujące okienka.
- Dr.Web Cloud – natychmiastowa reakcja na nowe zagrożenia*.
- Proaktywna ochrona przeciwko nieznanym zagrożeniom poprzez uniemożliwienie modyfikacji krytycznych obiektów systemu Windows oraz kontrolowanie niebezpiecznych działań*.
- Skanowanie w tle i aktywny podsystem neutralizowania zagrożeń – Dr.Web 8.0 dla Windows potrafi wyeliminować każde zagrożenie, niezależnie od tego jak bardzo jest ono odporne na usunięcie.
- W ramach sieci lokalnej, antywirus Dr.Web dla Windows może być kontrolowany z poziomu każdego komputera podłączonego do sieci LAN, bez instalowania Centrum Zarządzania Dr.Web.
- Szybkie/Pełne/Wybiórcze skanowanie pamięci RAM, dysków logicznych, płyt CD, dysków sieciowych, katalogów, plików, plików e-mail i innych obiektów w systemie

Wymagania systemowe

- Procesor: wspomagający system poleceń i686 i starszy.
- System operacyjny: Windows Server 2000** / 2003 (x32 i x64**) / 2008 / 2012 (x64)
- Pamięć operacyjna: 512 MB i więcej.

Przydatne linki

Opis: http://products.drweb.com/fileserver/win

---

* Dostępne dla Windows Server 2008 i późniejszych wersji.

** Tylko dla wersji 7.0.

Dr.Web dla Mac OS X Server

Ochrona antywirusowa stacji roboczych sterowanych przez wersje serwerowe OS Mac

Funkcje kluczowe

- Skanowanie obiektów autouruchamiania, wymiennych nośników informacji, dysków sieciowych i logicznych, formatów pocztowych, plików i katalogów, włącznie z tymi zapakowanymi i znajdującymi się w archiwach.
- Szybkie skanowanie pełne i fragmentaryczne.
- Skanowanie antywirusowe ręczne, automatyczne lub na podstawie wcześniej stworzonego harmonogramu.
- Ochrona regulacji monitora SpIDerGuard® za pomocą hasła chroniącego przed nieautoryzowanymi zmianami.
- Stosowanie czynności wobec zainfekowanych i podejrzanych obiektów oraz obiektów innego rodzaju, łącznie z leczeniem, przeniesieniem do kwarantanny i usunięciem, w tym również wtedy, gdy wybrana wcześniej czynność okazała się niemożliwą do wykonania.
- Wyłączenie ze skanowania ścieżek i plików na życzenie użytkownika.
- Wykrywanie i usuwanie wirusów ukrytych w formatach nieznanych programów do pakowania.
- Rejestrowanie czasu zdarzenia, obiektu skanowania i rodzaju podjętego w związku z nim działania.
- Instalacja aktualizacji: automatyczna (zgodnie z harmonogramem) lub na żądanie.
- Automatyczne powiadomienie (w tym z użyciem powiadomień dźwiękowych) o zdarzeniach wirusowych.
- Izolacja zainfekowanych plików w kwarantannie z możliwością zaprogramowania czasu przechowywania obiektów w kwarantannie i jej maksymalnego rozmiaru.
- Leczenie, odzyskiwanie lub usuwanie obiektów przeniesionych do kwarantanny.
- Prowadzenie szczegółowego raportu pracy.
- Dostępność modułów w formie narzędzi wiersza polecenia, z możliwością ich integracji z Apple Scripts używanymi do obsługi systemu.

Zalety

- Komfortowe Centrum zarządzania.
- Duża szybkość skanowania.
- Możliwość tworzenia własnych profili skanowania.
- Niezawodna ochrona w czasie rzeczywistym.
- Minimalne obciążenie chronionego systemu.
- Niewielki ruch sieciowy przy aktualizacjach.
- Różnorodne konfiguracje.
- Łatwość zarządzania.
- Nowoczesny i wygodny interfejs.

Wymagania systemowe

- Mac OS X Server 10.4 lub w wyższej wersji.
- Procesor Intel.
- 128 MB pamięci operacyjnej.
- 120 MB wolnego miejsca na dysku.
- Dostęp do sieci internetowej: w celu dokonania rejestracji i uzyskania aktualizacji.

Przydatne linki

Opis: http://products.drweb.com/fileserver/mac

Dr.Web dla serwerów Novell NetWare

Ochrona antywirusowa magazynów plików

Funkcje kluczowe

- Skanowanie sektorów serwera zgodnie z planem lub na żądanie administratora. Skanowanie „na bieżąco" wszystkich plików przechodzących przez serwer. Skanowanie wielowątkowe.
- Możliwość regulacji stopnia obciążenia procesora, co pozwala przyznać priorytet procesowi skanowania w systemie.
- Automatyczne odłączanie od serwera stacji będącej źródłem zagrożenia wirusowego.
- Protokołowanie skanowania; regulowanie stopnia uszczegółowienia protokołu.
- Powiadomienia o wykryciu zainfekowanych obiektów.
- Leczenie, usuwanie lub przeniesienie zainfekowanych obiektów do kwarantanny.
- Zarządzanie antywirusem za pomocą konsoli serwera lub zdalnej konsoli.
- Prowadzenie statystyki skanowania i dziennika czynności antywirusa.
- Automatyczne aktualizacje baz wirusów.

Zalety

- Najszersze spektrum wspomaganych wersji Novell NetWare – od 3.12 do 6.5. Wsparcie obszaru nazw NetWare.
- Duża prędkość skanowania wielkich zbiorów danych przy minimalnym obciążeniu systemu operacyjnego.
- Prosta instalacja.
- Elastyczny, zorientowany na klienta system konfiguracji parametrów skanowania i czynności z wykrytymi złośliwymi obiektami.

Wymagania systemowe

- Novell NetWare w wersji 3.12-6.5 z zainstalowanymi dodatkami z Minimum patch list
- 25 MB pamięci operacyjnej + 25 MB pamięci operacyjnej dla każdego dodatkowego procesu skanowania.
- 20 MB miejsca na dysku.

Przydatne linki

Opis: http://products.drweb.com/fileserver/novell

Dr.Web dla serwerów Unix

Ochrona antywirusowa magazynów plików

Zalety

- Duża efektywność i stabilność pracy.
- Duża prędkość skanowania przy minimalnym obciążeniu systemu operacyjnego, dzięki czemu Dr.Web może doskonale funkcjonować na serwerach o praktycznie dowolnej konfiguracji.
- Elastyczny, zorientowany na klienta system konfiguracji – wybór obiektów do skanowania, czynności z wykrytymi wirusami lub podejrzanymi plikami.
- Doskonała kompatybilność – pasuje do znanych ekranów międzysieciowych i monitorów plików.
- Komfort administrowania, prosta instalacja i konfiguracja.

Funkcje kluczowe

- Skanowanie sektorów serwera zgodnie z ustalonym wcześniej planem lub na żądanie administratora.
- Skanowanie „na bieżąco" – bezpośrednio podczas zapisywania lub otwierania plików na serwerze ze stacji roboczych.
- Skanowanie wielowątkowe.
- Automatyczne odłączanie od serwera stacji będącej źródłem zagrożenia wirusowego.
- Błyskawiczne informowanie administratora oraz innych użytkowników i grup o incydentach wirusowych – pocztą elektroniczną lub poprzez wysłanie powia-domień na telefon komórkowy lub pager.
- Izolacja zainfekowanych plików w kwarantannie.
- Leczenie, odzyskiwanie i/lub usuwanie plików z kwarantanny.
- Prowadzenie dziennika czynności antywirusa.
- Automatyczne aktualizacje baz wirusów.

Wymagania systemowe

- Samba 3.0 i w wyższej wersji.

Wspierane systemy operacyjne

- Dystrybucje Linux, posiadające jądro w wersji 2.4.x i wyższej.
- FreeBSD w wersji 6.x i wyższej dla platformy Intel x86
- Solaris w wersji 10 dla platformy Intel x86

Przydatne linki

Opis: http://products.drweb.com/fileserver/unix

Dr.Web dla Novell Storage Services

Ochrona antywirusowa magazynów plików

Zalety

- Duża efektywność i stabilność pracy.
- Duża prędkość skanowania przy minimalnym obciążeniu systemu operacyjnego, dzięki czemu Dr.Web® dla Novell Storage Services może doskonale funkcjonować na serwerach o praktycznie dowolnej konfiguracji.
- Elastyczny system konfiguracji – wybór obiektów do skanowania, czynności z wykrytymi wirusami lub podejrzanymi plikami.
- Doskonała kompatybilność – pasuje do znanych ekranów międzysieciowych i monitorów plików.
- Komfort w administrowaniu.
- Prosta instalacja i konfiguracja.

Funkcje kluczowe

- Możliwość leczenia lub usuwania wszelkich typów złośliwych obiektów.
- Skanowanie asynchroniczne – podczas zapisywania lub otwierania plików na serwerze ze stacji roboczych.
- Skanowanie wielowątkowe.
- Scentralizowane gromadzenie danych statystycznych, uwzględniających wszystkie aspekty pracy systemu.
- Powiadamianie administratora o wynikach skanowania pocztą elektroniczną za pomocą szablonów opisanych w systemie, co pozwala otrzymywać informacje w najdogodniejszej formie.
- Izolacja zainfekowanych i podejrzanych plików w kwarantannie.
- Leczenie, odzyskiwanie i/lub usuwanie plików z kwarantanny.
- Prowadzenie dziennika czynności antywirusa.
- Ochrona własnych modułów przed awariami.
- Automatyczne aktualizacje baz wirusów.

Wymagania systemowe

- Novell Open Enterprise Server SP2 na bazie systemu operacyjnego SUSE Linux Enterprise Server 10 SP3.
- Zainstalowany serwis Novell Storage Services (NSS).
- System plików NSS, zamontowany w określonym katalogu systemu.
- Nie mniej niż 300 MB wolnego miejsca na dysku na zainstalowanie produktu.
- Pozostałe wymagania systemowe są zgodne z wymaganiami systemu operacyjnego SUSE Linux Enterprise Server 10 SP3.

Wspierane systemy operacyjne

- SUSE Linux Enterprise Server 10 SP3.

Przydatne linki

Opis: http://products.drweb.com/fileserver/nss

Dr.Web Mail Security Suite

Ochrona poczty

- Dr.Web dla serwerów pocztowych Unix – certyfikowany przez FSKTiE Rosji
- Dr.Web dla MS Exchange – certyfikowany przez FSKTiE Rosji
- Dr.Web dla IBM Lotus Domino (Windows, Linux)
- Dr.Web dla serwerów pocztowych Kerio (Windows, Linux)

Wspierane systemy operacyjne

Produkt Dr.Web	Windows	Linux	FreeBSD	Solaris
		dla platformy Intel x86		
Dr.Web dla serwerów pocztowych Unix		z jądrem w wersji 2.4.x i wyższej.	w wersji 6.x i wyższej	w wersji 10
Dr.Web dla MS Exchange	Server 2000 / 2003 / 2008			
Dr.Web dla IBM Lotus Domino	Server 2000 / 2003 / 2008 / 2008 R2 (wersje 32- i 64- bitowe)	Red Hat Enterprise Linux (RHEL) w wersji 4 i 5, Novell SuSE Linux Enterprise Server (SLES) w wersji 9 i10 (tylko 32-bitowe)		
Dr.Web dla serwerów pocztowych Kerio	Server 2000 / 2003 / 2008 XP / Vista / 7	Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Licencjonowanie Dr.Web Mail Security Suite

Rodzaje licencji

- Pod względem liczby chronionych użytkowników (jest ona nieograniczona).
- Licencja serwerowa – do skanowania nieograniczonej ilości korespondencji na jednym serwerze, z maksymalnie 3000 chronionych użytkowników.

Produkty programowe Dr.Web do ochrony poczty można nabyć oddzielnie lub w zestawie typu Dr.Web Enterprise Security Suite. W drugim przypadku udzielana jest dodatkowo licencja na Centrum zarządzania Dr.Web Enterprise Security Suite, Antyspam i SMTP proxy.

Jednoczesne używanie produktów do ochrony poczty i komponentu dodatkowego SMTP proxy nie tylko istotnie zwiększa ogólne bezpieczeństwo sieci, ale i zmniejsza obciążenie wewnętrznych serwerów pocztowych i stacji roboczych.

Wersje licencji

	Dr.Web dla MS Exchange	**Dr.Web dla IBM Lotus Domino**	**Dr.Web dla serwerów pocztowych Unix**	**Dr.Web dla serwerów pocztowych Kerio**
Licencja bazowa	Antywirus			
Dodatkowe komponenty				
Antyspam	+	+	+	
SMTP proxy	+	+	+	+
Centrum zarządzania	+	+	+	+

Produkty Dr.Web do ochrony poczty dostępne są również w zestawach ekonomicznych Dr.Web dla małych i średnich przedsiębiorstw.

Dr.Web dla serwerów pocztowych i bram Unix

Ochrona antywirusowa i antyspamowa ruchu pocztowego w sieci, przechodzącego przez serwery sterowane przez UNIX (Linux/FreeBSD/Solaris(x86))

Funkcje kluczowe

- Filtracja wiadomości pocztowych pod kątem wirusów i spamu.
- Rozpakowanie wiadomości pocztowych i analiza wszystkich ich komponentów.
- Prawidłowa obsługa większości znanych rodzajów archiwów, w tym wielotomowych i samorozpakowujących się (SFX).
- Białe i czarne listy.
- Konfigurowalne powiadomienia.
- Prowadzenie statystyki, uwzględniającej wszystkie aspekty pracy systemu.
- Ochrona pracy własnych modułów przed uszkodzeniami.

Zgodność z wymaganiami prawa rosyjskiego

Dla serwerów pocztowych UNIX Dr.Web posiada certyfikaty zgodności FSKTiE i FSB. Dzięki temu produkty mogą być wykorzystywane w organizacjach wymagających podwyższonego poziomu bezpieczeństwa, w tym produkty w zestawie podsystemu ochrony antywirusowej w systemach informatycznych danych osobowych (SIDO) klasy K1. Możliwość archiwizowania wszystkich wiadomości pocztowych pozwala również stosować produkt w zestawie systemów informacyjnych instytucji kredytowych.

Możliwość elastycznej konfiguracji na potrzeby użytkowników

Do konfigurowania Dr.Web dla serwerów pocztowych UNIX można stosować reguły. To znacznie podwyższa elastyczność produktu i korzystnie odróżnia go od konkurencyjnych odpowiedników, do konfiguracji których używane są parametry statystyczne pliku konfiguracyjnego. Filtracja i zmiana wiadomości następuje w zależności od posiadanych polityk. Przy czym administrator może nadawać oddzielne reguły obsługi nie tylko dla różnych użytkowników i grup, ale i w rzeczywistości dla każdego listu. Dzięki temu produkt jest w stanie spełniać wszelkie wymagania korporacyjne odnośnie do poziomu bezpieczeństwa informacyjnego, co jest niezwykle ważne w świetle obowiązującej ustawy o ochronie danych osobowych.

Brak wysokich wymagań co do kwalifikacji administratora

Mimo bogactwa możliwości funkcjonalnych, Dr.Web dla serwerów pocztowych UNIX nie wymaga długotrwałej konfiguracji przed wprowadzeniem do eksploatacji. Ponadto jest on dostarczany nie tylko jako produkt programowy, ale i w zestawie programowo-sprzętowym Dr.Web Office Shield – serwera, zaprojektowanego do pracy na zasadzie „zainstalowane i zapomniane".

Duża prędkość odpowiedzi

Technologia skanowania wielowątkowego zapewnia dużą szybkość odpowiedzi systemu. Wiadomości skanowane są zawsze „na bieżąco", równolegle z obsługą wcześniej przyjętych plików. Dzięki temu użytkownicy końcowi mogą odbierać korespondencję praktycznie w mgnieniu oka.

Dodatkowe zalety Antyspamu Dr.Web:

- nie wymaga przeszkolenia i zaczyna efektywnie działać od momentu instalacji – w odróżnieniu od antyspamów, zbudowanych z wykorzystaniem algorytmu Bayesa (Panda, Kaspersky);
- podjęcie decyzji o tym, czy dana wiadomość zostanie zakwalifikowana jako spam czy nie, nie zależy od języka wiadomości;
- pozwala określać różne czynności dla różnych kategorii spamu;

- wykorzystuje własne czarne i białe listy, co nie daje możliwości nadwyrężenia wizerunku firmy poprzez złośliwe wpisanie jej na listę niechcianych adresów;
- dopuszcza rekordowo małą liczbę błędnej kwalifikacji;
- wymaga aktualizacji nie częściej niż jeden raz na dobę – dzięki unikalnym technologiom rozpoznawania niechcianej poczty w oparciu o kilka tysięcy reguł nie ma konieczności pobierania częstych aktualizacji.

Ochrona informacji poufnej

Produkt pozwala odzyskiwać wiadomości, usunięte przez użytkowników ze swoich skrzynek pocztowych przez przypadek, a także prowadzić śledztwa związane z wyciekiem informacji. Sprzyja temu możliwość zarządzania kwarantanną zarówno przez interfejs sieciowy, jak i poprzez specjalne narzędzie, a także możliwość archiwizacji wszystkich przechodzących wiadomości.

Komfort w administrowaniu

Możliwość korzystania z interfejsu sieciowego w celu konfiguracji i zarządzania produktem umożliwia łatwe administrowanie ochroną z dowolnego miejsca na świecie.

Otwartość

Dr.Web dla serwerów pocztowych UNIX daje się zintegrować z rozwiązaniami innych producentów. Ponadto dzięki otwartemu API można do niego dodać nowe możliwości funkcjonalne.

Możliwość podłączenia nieograniczonej liczby dodatków

Dr.Web dla serwerów pocztowych UNIX pozwala zwiększać funkcjonalność w nieograniczonym stopniu, a przy tym każdy opracowany dodatek współpracuje od razu ze wszystkimi obsługiwanymi serwerami poczty elektronicznej. Obsługiwane dodatki:

- **Dr.Web** – dodatek antywirusowej kontroli poczty za pomocą silnika antywirusowego Dr.Web;
- **vaderetro** – dodatek filtrujący pocztę pod kątem spamu przez własną bibliotekę VadeRetro.
- **headersfilter** – dodatek filtrujący wiadomości według nagłówków.

Wspierane systemy operacyjne

- Dystrybucje Linux, posiadające jądro w wersji 2.4.x i wyższej.
- FreeBSD w wersji 6.x i wyższej dla platformy Intel x86.
- Solaris w wersji 10 dla platformy Intel x86.

Dr.Web SMTP proxy

Moduł Dr.Web SMTP proxy – komponent produktu Dr.Web dla serwerów pocztowych Unix – może być zainstalowany zarówno w zdemilitaryzowanej strefie (DMZ), jak i wewnątrz systemu pocztowego. Dzięki temu, że serwer kontroli wiadomości pocztowych może być przeniesiony do strefy zdemilitaryzowanej, a serwer pocztowy – izolowany od Internetu, nawet w przypadku włamania do serwera przestępca internetowy nie dostanie się do ważnych dla firmy informacji. Rozwiązanie zapewnia pełną kontrolę korespondencji zgodnie z protokołami SMTP/LMTP

Wykorzystanie Dr.Web SMTP proxy:

- istotnie zwiększa ogólne bezpieczeństwo sieci;
- umożliwia znaczną poprawę jakości filtrowania, gdyż nie ma ograniczeń nakładanych przez serwery pocztowe;
- zmniejsza obciążenia wewnętrznych serwerów pocztowych i stacji roboczych;
- zwiększa stabilność działania systemu kontroli poczty jako całości.

Zalety

Ochrona przed atakami spamerów – za pomocą Dr.Web SMTP proxy administrator zyskuje możliwość ograniczania parametrów sesji SMTP, a tym samym określania cech ataku spamerów.

Weryfikacja autentyczności adresu IP – Dr.Web SMTP proxy umożliwia organizację weryfikacji autentyczności adresu IP i ochrony firmy przed spamem, zamaskowanym pod niewiarygodnym adresem IP nadawcy.

Ochrona przed atakami hakerów – Dr.Web SMTP proxy pozwala na skuteczną obronę zarówno przed pasywnymi atakami (typu PLAIN, LOGIN, itd.), jak i atakami aktywnymi bez sortowania ze słownikiem.

Ochrona przed pułapkami spamowymi – Dr.Web SMTP proxy pozwala na sprawdzenie odbiorcy pod kątem pułapki spamowej.

Ochrona przed nieprawidłowo sporządzonymi listami – Dr.Web SMTP proxy pozwala na blokowanie listów z pustymi polami nadawcy, a jednocześnie na prawidłową obsługę listów od klientów poczty, którzy niepoprawnie sporządzają listy.

Oszczędność ruchu w Internecie – korzystanie z Dr.Web SMTP proxy pozwala na oszczędność ruchu w Internecie i na blokowanie wysyłania załączników o bardzo dużych rozmiarach przez pracowników firm.

Ograniczenie serwerów Open Relays – jeśli w firmie istnieje produkcyjna konieczność organizacji takiego serwera, administrator może za pomocą Dr.Web SMTP proxy ograniczyć spis domen, na które wysyłanie listów jest dozwolone.

Przydatne linki

Opis: http://products.drweb.com/mailserver/maild

Dr.Web dla MS Exchange

Antywirusowe i antyspamowe skanowanie ruchu w sieci, przekazywanego przez serwery pocztowe MS Exchange 2000/2003/2007/2010

Zalety

- Możliwość wykorzystania w organizacjach wymagających podwyższonego poziomu bezpieczeństwa – produkt całkowicie spełnia wymagania prawa rosyjskiego i posiada certyfikaty zgodności Federalnej Służby Kontroli Technicznej i Eksportowej oraz Federalnej Służby Bezpieczeństwa.
- Duże możliwości instalacji i precyzyjnej konfiguracji w zależności od potrzeb firmy.
- Duża prędkość skanowania przy minimalnym obciążeniu systemu operacyjnego, dzięki czemu Dr.Web może doskonale funkcjonować na serwerach o praktycznie dowolnej konfiguracji.
- Wsparcie koncepcji zadań serwera i agentów transportowych dla MS Exchange Server 2007/2010 – skanowanie listów pod kątem obecności wirusów i spamu może być dokonywane zarówno na poziomie transportowym, jaki i na poziomie wsparcia interfejsu antywirusowego VSAPI. Dzięki temu zapewniony jest optymalny poziom ochrony organizacji.
- Wbudowany antyspam, niewymagający przeszkolenia (działa od momentu instalacji), który istotnie zmniejsza obciążenie serwera i zwiększa wydajność pracy pracowników firmy.
- Możliwość filtracji zgodnie z czarnymi i białymi listami, co pozwala zarówno wyłączyć ze skanowania określone adresy, jak i zwiększać jego wydajność.
- Nowa możliwość elastycznego konfigurowania parametrów ochrony aplikacji przez przeglądarkę w dogodnym dla użytkownika trybie, za pomocą konsoli sieciowej administratora.
- Możliwość filtracji według rodzajów plików, co pozwala firmie zmniejszyć wielkość ruchu sieciowego.
- Obecność mechanizmu grupowania, dzięki któremu możliwe jest określanie różnych parametrów dla różnych grup pracowników, co istotnie skraca uruchamianie systemu ochrony antywirusowej i ułatwia zarządzanie produktem Dr.Web.
- Duża wydajność i stabilność pracy dzięki funkcji skanowania wielowątkowego.
- Unikalne technologie wykrywania nieznanych (najnowszych) programów do pakowania i złośliwych obiektów.
- W pełni automatyczne uruchamianie aplikacji (przy starcie systemu).
- Wygodny system aktualizacji za pomocą harmonogramu zadań Windows.
- Wyczerpująca dokumentacja techniczna.

Funkcje kluczowe

- Antywirusowe i antyspamowe skanowanie wiadomości pocztowych, w tym załączonych plików, w czasie rzeczywistym.
- Antywirusowy monitoring wiadomości w skrzynkach pocztowych użytkowników oraz plików w katalogach ogólnego dostępu.
- Antywirusowa kontrola tranzytowego strumienia poczty, przechodzącego przez serwer MS Exchange.
- Leczenie zainfekowanych plików.
- Grupowanie użytkowników za pomocą Active Directory.
- Wsparcie koncepcji zadań serwera i agentów transportowych dla MS Exchange Server 2007/2010.
- Skanowanie z zastosowaniem wyznaczonych parametrów: wybór maksymalnego rozmiaru i typów skanowanych obiektów, czynności (w tym również dla plików, niepoddających się kontroli), a także sposobów obsługi zainfekowanych obiektów.
- Wykrywanie złośliwych obiektów w wielokrotnie zarchiwizowanych plikach.

- Stosowanie różnych czynności w zależności od rodzaju spamu, włącznie z przeniesieniem do kwarantanny i dodaniem prefiksu do tematu wiadomości.
- W razie konieczności – dodawanie dowolnych tekstów do odsyłanych wiadomości.
- Izolacja zainfekowanych i podejrzanych plików w kwarantannie.
- Powiadomienie administratora lub innych użytkowników o incydentach wirusowych.
- Prowadzenie statystyki pracy zestawu Dr.Web.
- Automatyczne aktualizacje.

Wymagania systemowe

Przy korzystaniu z Microsoft Exchange Server 2000/2003:

- Procesor Pentium 133 MHz (zaleca się 733 MHz).
- Pamięć operacyjna: 256 MB (zaleca się 512 MB).
- Wolne miejsce na dysku: 20 MB na instalację; 50 MB na dziennik zdarzeń.
- Microsoft® Windows® 2000 Server lub Advanced Server z zainstalowanym SP4; Microsoft® Windows® Server 2003 (wersja Standard, Enterprise lub Datacenter) z zainstalowanym SP1 lub wyżej.

Przy korzystaniu z MS Exchange Server 2007/2010:

- Procesor Intel z architekturą x64 i wsparciem technologii Intel 64 lub AMD ze wsparciem platformy AMD64.
- Pamięć operacyjna: 2 GB.
- Wolne miejsce na dysku: 20 MB na instalację; 50 MB na dziennik zdarzeń.
- Microsoft® Windows® Server 2003 R2 x64 z zainstalowanym SP2; Microsoft® Windows® Server 2008 x64.

Przydatne linki

Opis: http://products.drweb.com/mailserver/exchange

Dr.Web dla IBM Lotus Domino

Ochrona antywirusowa i antyspamowa platformy IBM Lotus Domino sterowanej przez Windows i Linux

Zalety

- **Minimalny łączny koszt**

Dr.Web dla IBM Lotus Domino działa nie tylko w oddzielnie stojących serwerach, ale i w serwerach partycji oraz klastrach Lotus Domino. Kopie antywirusów w różnych sekcjach występują w pamięci komputera autonomicznie, wykorzystując bazy ogólne i pliki wykonywalne. W tym przypadku licencjonować należy tylko jedną kopię, co istotnie zmniejszy koszty ochrony antywirusowej.

- **Ready for IBM Lotus software**

Dr.Web dla IBM Lotus Domino jest wprowadzony do katalogu rozwiązań IBM Lotus Business Solutions Catalog i posiada znak Ready for IBM Lotus Software. Znak ten potwierdza zgodność produktu z systemem Lotus Domino i świadczy o spełnieniu wszystkich wymagań na zgodność z IBM.

- **Duża szybkość skanowania**

Organizacja systemu Dr.Web dla IBM Lotus Domino, szczególna realizacja metody skanowania i możliwość elastycznego zarządzania tym procesem, pozwoliły osiągnąć bardzo dużą szybkość skanowania przy małym zużyciu zasobów systemowych.

- **Prosta instalacja i elastyczna konfiguracja**

Przewidziano automatyczne i łatwo sterowalne uruchamianie Dr.Web dla IBM Lotus Domino. Program obsługuje skrypty administracyjne i posiada szczegółową dokumentację. Komfort zarządzania zestawem jest zapewniony dzięki możliwości elastycznego konfigurowania przez konsolę administratora. Środki dokładnej konfiguracji algorytmów antywirusa na podstawie rezultatów skanowania pozwalają odsyłać powiadomienia o wykrytych wirusach nadawcy, odbiorcom i administratorom systemu, zachowywać nagłówki otrzymanych wiadomości pocztowych oraz załączników do nich, itp.

- **Komfort w administrowaniu**

Mechanizmy grupowania i zarządzanie grupami znacznie upraszczają administrowanie ochroną antywirusową.

Funkcje kluczowe

- Kontrola i filtracja wiadomości pocztowych oraz wszystkich ich komponentów pod kątem wirusów, spamu i niepożądanych wiadomości „na bieżąco" lub z polecenia administratora.
- Filtracja poczty pod kątem spamu, w tym według czarnych i białych list adresów.
- Skanowanie dokumentacji w wyznaczonych bazach nsf pod kątem obecności wirusów.
- Skanowanie obiektów na żądanie, za pomocą funkcji ręcznego uruchomienia i wstrzymania zadań skanera.
- Rozkład wiadomości pocztowych z wyodrębnieniem wszystkich ich komponentów do późniejszej analizy.
- Leczenie zainfekowanych wiadomości pocztowych i załączonych do nich plików.
- Wykrywanie złośliwych obiektów w wielokrotnie zarchiwizowanych plikach.
- Wykorzystanie mechanizmu wykrywania programów złośliwych, ukrytych przez nieznane programy do pakowania.
- Wykorzystanie dodatkowej technologii wykrywania nieznanych obiektów złośliwych, która zwiększa prawdopodobieństwo wykrycia najnowszych typów wirusów.
- Przechowywanie zainfekowanych i podejrzanych obiektów w kwarantannie (dostęp do przeniesionych do kwarantanny obiektów odbywa się przez klienta Lotus Notes).

- Powiadamianie o wynikach skanowania za pomocą szablonów opisanych w systemie, co pozwala adresatom, administratorom i innym osobom uzyskiwać informacje w najdogodniejszej formie.
- Prowadzenie statystyki pracy systemu.
- Ochrona pracy własnych modułów przed uszkodzeniami.
- Automatyczne aktualizacje.

Wspierane systemy operacyjne

- Wersja dla Windows: Windows Server 2000/2003/2008/2008R2 (wersje 32- i 64-bitowe).
- Wersja dla Linux: Red Hat Enterprise Linux (RHEL) w wersji 4 i 5, Novell SuSE Linux Enterprise Server (SLES) w wersji 9 i10 (tylko 32-bitowe)

Przydatne linki

Opis: http://products.drweb.com/lotus

Dr.Web dla serwerów pocztowych Kerio

Skanowanie antywirusowe załączników wszystkich wiadomości pocztowych, przekazywanych zgodnie z protokołami SMTP/POP3

Zalety

- Doskonała kompatybilność z serwerami pocztowymi Kerio, potwierdzona testami Kerio Technologies.
- Możliwość pracy w trybie scentralizowanej ochrony za pomocą Centrum zarządzania Dr.Web Enterprise Security Suite.
- Dr.Web – obecnie jedyny rosyjski dodatek antywirusowy dla serwerów pocztowych Kerio, co jest niezwykle ważne przy dostarczaniu produktu przedsiębiorstwom państwowym.
- Wsparcie użytkowników ze względu na lokalizację, np. w Polsce - w języku polskim
- Minimalny czas dostarczania wiadomości i większa niezawodność produktu dzięki wykorzystaniu technologii skanowania wielowątkowego.
- Minimalne wymagania systemowe, bez obciążeń sieci lokalnej.
- Elastyczny, zorientowany na klienta system konfiguracji – wybór obiektów do skanowania i czynności z wykrytymi wirusami lub podejrzanymi plikami.
- Możliwość wyboru czynności wobec plików niepoddających się skanowaniu.
- Komfortowe zarządzanie z konsoli administracyjnej serwera pocztowego Kerio.

Funkcje kluczowe

- Kontrola załączników plikowych wszystkich wchodzących i wychodzących wiadomości elektronicznych.

Wspierane systemy operacyjne

- Wersja dla Windows: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/ (wersje 32-i 64-bitowe).
- Wersja dla Linux: Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 i 11.1; CentOS Linux 5.2 i 5.3; Debian 5.0; Ubuntu 8.04 LTS.

Przydatne linki

Opis: http://products.drweb.com/mailserver/kerio

Dr.Web Gateway Security Suite

Ochrona bram pocztowych i internetowych

- Dr.Web dla bram internetowych Unix – certyfikowany przez FSKTiE Rosji
- Dr.Web dla bram internetowych Kerio
- Dr.Web dla MIMEswepper
- Dr.Web dla Qbik WinGate

Wspierane systemy operacyjne

	Windows	Linux	FreeBSD	Solaris
		dla platformy Intel x86		
Dr.Web dla bram internetowych Unix		z jądrem w wersji 2.4.xi wyższej.	w wersji 6.x i wyższej	w wersji 10
Dr.Web dla bram internetowych Kerio	2000 / XP / 2003 / 2008 / 7			
Dr.Web dla MIMEsweeper	2000 Server SP4 lub w wyższej wersji/ Server 2003 lub w wyższej wersji			
Dr.Web dla Qbik WinGate	Vista / Server 2008 / Server 2003 / XP / 2000 (systemy 32- i 64-bitowe)			

Licencjonowanie Dr.Web Gateway Security Suite

Rodzaje licencji

- Pod względem liczby chronionych użytkowników (jest ona nieograniczona).
- Licencja serwerowa – do skanowania nieograniczonego ruchu w sieci na jednym serwerze, z maksymalnie 3000 chronionych użytkowników.

Produkty programowe Dr.Web do ochrony bram można nabyć oddzielnie lub w zestawie Dr.Web Enterprise Security Suite. W drugim przypadku udzielana jest dodatkowo licencja na Centrum zarządzania Dr.Web Enterprise Security Suite (dla bram internetowych Kerio i Unix) i Antyspam (oprócz bram internetowych Unix i Kerio).

Wersje licencji

	Dr.Web dla bram inter-netowych Unix	Dr.Web dla bram inter-netowych Kerio	Dr.Web dla MIME-sweeper	Dr.Web dla Qbik WinGate
Licencja bazowa	Antywirus			
Dodatkowe komponenty				
Antyspam			+	+
Centrum zarządzania	+	+		

Produkty Dr.Web do ochrony bram dostępne są również w zestawach ekonomicznych Dr.Web dla małych i średnich przedsiębiorstw.

Dr.Web dla bram internetowych Unix

Skanowanie antywirusowe ruchu sieciowego HTTP i FTP, przechodzącego przez korporacyjną bramę internetową – serwer proxy

Funkcje kluczowe

- Skanowanie antywirusowe ruchu sieciowego FTP i HTTP.
- Scentralizowane zarządzanie przez sieciowego administratora Centrum zarządzania Dr.Web Enterprise Security Suite.
- Filtracja dostępu według typu MIME i rozmiaru plików lub według nazwy hosta.
- Regulacja dostępu do zasobów sieciowych.
- Optymalizacja kontroli ruchu w sieci dzięki korzystaniu z technologii Preview.
- Praca zarówno z protokołem IPv4, jak i z protokołem następnej generacji IPv6.
- Kontrola i stosowanie odpowiednich czynności w zależności od typów skanowanych plików.
- Izolacja zainfekowanych obiektów w kwarantannie.
- Dostarczenie raportu w dogodnej formie.
- Obsługa kilku zapytań w trakcie jednego połączenia.
- Ochrona przed nieautoryzowanym dostępem.
- Monitoring i automatyczne przywrócenie pracy systemu.
- Powiadomienie użytkownika o próbach załadowania złośliwej strony lub o wykryciu wirusa.

Zalety

- Szerokie możliwości organizacji kompleksowej ochrony przed zagrożeniami, ukrytymi we wchodzącym ruchu sieciowym
- Dostawa tylko bezpiecznych treści do wnętrza chronionej sieci
- Skuteczna filtracja ruchu w sieci na poziomie serwera ICAP – praktycznie bez zwalniania szybkości dostarczenia treści.
- Znaczące zmniejszenie kosztów korzystania z sieci internetowej.
- Skuteczne przeciwdziałanie przenikaniu złośliwych programów dowolnego typu
- Wysoka skalowalność – zdolność do opracowywania bardzo dużych zbiorów informacji w czasie rzeczywistym.
- Doskonała zgodność – integracja z dowolnym oprogramowaniem, wspomagającym protokół ICAP, ze wszystkimi znanymi ekranami międzysieciowymi.
- Wsparcie praktycznie wszystkich wykorzystywanych obecnie systemów operacyjnych na bazie Unix.
- Brak wysokich wymagań wobec zasobów systemowych – produkt funkcjonuje doskonale na bramach internetowych o praktycznie dowolnej konfiguracji.
- Elastyczność i komfort administrowania – produkt pozwala realizować takie schematy ochrony, które odpowiadają polityce bezpieczeństwa firmy.

Wspierane systemy operacyjne

- Linux z jądrem w wersji 2.4.x i wyższej.
- FreeBSD w wersji 6.x i wyższej (dla platformy Intel x86).
- Solaris w wersji 10 (dla platformy Intel x86).
- Dowolne serwery proxy, doskonale wspomagające protokół ICAP, w szczególności:
- Squid w wersji co najmniej 3.0.;
- Shweby w wersji co najmniej 1.0.;
- SafeSquid w wersji co najmniej 3.0.

Przydatne linki

Opis: http://products.drweb.com/gateway/unix

Dr.Web dla bram internetowych Kerio

Antywirusowe skanowanie ruchu w sieci, przekazywanego zgodnie z protokołami HTTP, FTP, SMTP i POP3, a także za pośrednictwem usługi sieciowej Kerio Clientless SSLVPN

Dr.Web dla bram internetowych Kerio – dodatek antywirusowy, który podłącza się do ekranu międzysieciowego Kerio. Instaluje się go na tym samym komputerze, na którym jest zainstalowany Kerio i wykorzystywany jest przez Kerio jako zewnętrzne oprogramowanie antywirusowe.

Zalety

- Wykrywanie złośliwych obiektów, przekazywanych według protokołów HTTP, FTP, SMTP i POP3, a także za pośrednictwem usługi sieciowej Kerio Clientless SSLVPN.
- Solidne zabezpieczenie dostępu do Internetu zarówno prywatnym użytkownikom, jak i firmom różnej wielkości i o różnym rodzaju działalności.
- Możliwość pracy w trybie scentralizowanej ochrony za pomocą Centrum zarządzania Dr.Web Enterprise Security Suite.
- Komfort administrowania – możliwość otrzymywania wiadomości o wszystkich incydentach wirusowych zarówno przez powiadomienia pocztowe, jak i przez SMS.
- Minimalny czas dostarczania wiadomości dzięki skanowaniu wielowątkowemu.

Funkcje kluczowe

- Wykrywanie złośliwych obiektów, przekazywanych według protokołów HTTP, FTP, SMTP i POP3, a także za pośrednictwem usługi sieciowej Kerio Clientless SSLVPN.
- Wykrywanie zainfekowanych załączników w listach elektronicznych i ich obsługa przez serwer pocztowy.
- Tworzenie listy sprawdzanych protokołów wymiany danych.
- Przegląd informacji o pracy programu przez konsolę web.
- Skanowanie z możliwością konfiguracji parametrów: wybór maksymalnego rozmiaru, typów skanowanych obiektów, sposobów obsługi zainfekowanych plików.
- Zastosowanie czynności wobec wykrytych zagrożeń zgodnie z konfiguracjami Kerio.
- Uruchomienie / zatrzymanie wykrywania złośliwych programów (według ich typów).
- Rejestracja błędów i bieżących zdarzeń w dzienniku rejestracji zdarzeń (EventLog) i w dzienniku tekstowym.
- Rozsyłanie powiadomień pocztowych o różnych zdarzeniach wybranym użytkownikom.
- Automatyczne aktualizacje baz wirusów.

Wymagania systemowe

- Co najmniej 55 MB wolnego miejsca na dysku.
- System operacyjny Microsoft® Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (wersje 32- i 64-bitowe).
- Ekran międzysieciowy Kerio 6 lub w późniejszej wersji.

Przydatne linki

Opis: http://products.drweb.com/gateway/kerio

Dr.Web dla MIMEsweeper

Ochrona antywirusowa i antyspamowa pocztowego ruchu sieciowego, przechodzącego przez serwery filtrowania treści ClearSwiftMIMEsweeper

Zalety

Prosta instalacja i konfiguracja

Zintegrowane z Dr.Web dla MIMEsweeper środki konfiguracji – to mistrzowie tworzenia scenariuszy – dzięki nim można tworzyć automatycznie najbardziej aktualne scenariusze kontroli wiadomości (typ 1 według klasyfikacji ClearSwift).

Zgodność z DEP

Dr.Web dla MIMEsweeper wspomaga technologię zapobiegania wykonywaniu danych (Data Execution Prevention, DEP), która pozwala na dodatkowe skanowanie pamięci i zapobieganie uruchomienia kodu. Dzięki temu użytkownicy nie muszą zmieniać trybu pracy DEP – złośliwe programy nie będą w stanie wykorzystywać mechanizmu obsługi wyjątków Windows.

Elastyczne konfiguracje

Po wykryciu zainfekowanego obiektu próbuje się go wyleczyć lub, jeżeli nie została wybrana opcja leczenia, od razu się go usuwa. Jeżeli do wiadomości pocztowej załączonych jest kilka plików lub archiwów, unieszkodliwia się tylko zainfekowane załączniki. Po wykryciu wirusa w treści wiadomości filtr treści przenosi wiadomość do kwarantanny. „Zdrowe" wiadomości, pliki i archiwa przekazywane są adresatowi bez zmian. Złośliwe wiadomości, których dodatek dla Dr.Web nie jest w stanie neutralizować, po oznakowaniu przenoszone są domyślnie do kwarantanny.

Funkcje kluczowe

- Skanowanie wiadomości pocztowych i ich załączników, w tym archiwów, i ich obsługa przez serwer pocztowy.
- Leczenie zainfekowanych obiektów.
- Izolacja zainfekowanych i podejrzanych plików w kwarantannie.
- Filtracja poczty pod kątem spamu, w tym z wykorzystaniem czarnych i białych list.
- Prowadzenie statystyki pracy zestawu.
- Automatyczne aktualizacje.

Wymagania systemowe

- Miejsce na twardym dysku: nie mniej niż 35 MB wolnego obszaru dyskowego.
- System operacyjny OC Windows 2000 Server z pakietem aktualizacji 4 (SP4) lub w wyższej wersji, lub Windows Server 2003 lub jeszcze późniejsza wersja.
- Pocztowy filtr treści ClearSwift MIME-sweeper™ dla SMTP 5.2 lub jeszcze późniejsza wersja.

Przydatne linki

Opis: http://products.drweb.com/mimesweeper

Dr.Web dla Qbik WinGate

Antywirusowe i antyspamowe skanowanie ruchu w sieci, przekazywanego zgodnie z protokołami HTTP/POP3/FTP serwera proxy i serwera SMTP QbikWinGate

Funkcje kluczowe

- Antywirusowe i antyspamowe skanowanie wiadomości pocztowych, przekazywanych zgodnie z protokołami SMTP i POP3, łącznie ze skanowaniem załączonych plików.
- Antywirusowe skanowanie plików i danych, przekazywanych zgodnie z protokołami HTTP i FTP.
- Leczenie zainfekowanych plików, przekazywanych zgodnie z protokołem HTTP.
- Dziennik rejestracji zdarzeń.
- Własny panel zarządzania i menedżer kwarantanny.
- Automatyczne aktualizacje baz wirusów.

Zalety

- Dr.Web dla Qbik WinGate – jedyny na chwilę obecną dodatek dla Qbik WinGate w rosyjskiej wersji językowej.
- Tylko Dr.Web dla Qbik WinGate posiada zarówno dokumentację, jak i wsparcie techniczne bezpośrednio od producenta.
- W odróżnieniu od konkurencyjnych odpowiedników, produkt firmy „Doctor Web" posiada możliwość filtracji antyspamowej. Wydajny i zwarty moduł antyspamowy nie wymaga przeszkolenia, pozwala określać różne czynności dla każdej z trzech przewidzianych przez program kategorii spamu oraz tworzyć czarne i białe listy adresów elektronicznych.
- Niemająca odpowiedników u innych producentów dodatkowa technologia wykrywania nieznanych obiektów złośliwych (Origins Tracing), również tych znajdujących się w archiwach nieznanego formatu.

Przydatne linki

Opis: http://products.drweb.com/gateway/qbik

Dr.Web Mobile Security Suite

Ochrona urządzeń mobilnych

- Dr.Web dla Symbian OS
- Dr.Web dla Windows Mobile
- Dr.Web dla Android

	Dr.Web dla Symbian OS	Dr.Web dla Windows Mobile	Dr.Web dla Android
Komponenty ochrony	Antywirus + Antyspam	Antywirus + Antyspam	Antywirus + Antyspam + Antyzłodziej
Scentralizowane zarządzanie w zestawie Dr.Web Enterprise Security Suite	–	+	+
Wspierane systemy operacyjne	Symbian Series60	Windows Mobile 2003 / 2003 SE / 5.0 / 6.0 / 6.1 / 6.5	Android OS: 2.1–4.2
Funkcje kluczowe			
Skanowanie w czasie rzeczywistym	+	+	+
Skanowanie plików, wchodzących przez GPRS/Infrared/ Bluetooth/podłączenia Wi-Fi/USB lub w czasie synchronizacji z PC	+	+	+
Dwa typy skanowania: pełne i wybiórcze	+	+	+
Możliwość włączenia / wyłączenia stałego skanowania karty pamięci	-	+	+
Skanowanie na żądanie całego systemu plików lub poszczególnych plików i katalogów	+	+	+
Skanowanie plików w archiwach ZIP, SIS, CAB, RAR	+	+	+
Czarne i białe listy wchodzących połączeń telefonicznych i wiadomości SMS	+	+	+
Usuwanie zainfekowanych plików	+	+	+

Przeniesienie podejrzanych plików do kwarantanny	+	+	+
Przywracanie plików z kwarantanny	+	+	+
Aktualizacje przez Internet: ■ zgodnie z protokołem HTTP z wykorzystaniem wbudowanego modułu GPRS; ■ za pośrednictwem połączenia Infrared / Bluetooth / Wi-Fi / USB; ■ za pomocą synchronizacji PC, posiadającego dostęp do sieci internetowej, poprzez podłączenie Active-Sync	+	+	+
Szczegółowe raporty o skanowaniu systemu	+	+	+
Zdalne sterowanie urządzeniem mobilnym w przypadku jego utracenia lub kradzieży – za pomocą aplikacji Antyzłodziej			+

Udzielanie licencji Dr.Web Mobile Security Suite

Licencje na Dr.Web Mobile Security Suite udzielane są według liczby chronionych urządzeń mobilnych.

Wersje licencji

Dr.Web dla Windows Mobile	Dr.Web dla Symbian OS	Dr.Web dla Android
■ Antywirus + Antyspam ■ Antywirus + Antyspam + Centrum zarządzania	■ Antywirus + Antyspam	■ Antywirus + Antyspam ■ Antywirus + Antyspam + Centrum zarządzania

Produkty Dr.Web dla urządzeń mobilnych dostępne są w zestawach ekonomicznych Dr.Web dla małych i średnich przedsiębiorstw.

Oferta specjalna

Użytkownicy Dr.Web Security Space i Dr.Web Antywirus mogą bezpłatnie korzystać z Dr.Web Mobile Security Suite.

Przydatne linki

Opis: http://products.drweb.com/mobile

Dr.Web Retail Security Suite.
Produkty dla klientów detalicznych

Dr.Web Security Space Pro
2PC / 1rok

Antywirus Dr.Web Pro
2PC / 1 rok

Dr.Web Bastion Pro
2PC / 1 rok

Nośnik flash 2 GB w prezencie

Dr.Web Security Space +
Antywirus Dr.Web dla Mac OS X
2 PC / 2 lata

Komplet „Mały biznes"
5 PC / 1 serwer / 1 rok

„Dr.Web Uniwersalny" (dla klientów ACS)

Pakiet medialny „Dr.Web Uniwersalny" jest dostarczany tylko przez Autoryzowane Centra Serwisowe Dr.Web i jest dostępny dla klientów ACS po specjalnej cenie.

Produkt zapewnia ochronę 1 PC i 1 urządzenia mobilnego przez okres 1 roku.

Skład licencji:

- Dr.Web Security Space
- Antywirus Dr.Web dla Mac OS X
- Antywirus Dr.Web dla Linux
- Dr.Web Mobile Security Suite
- Dr.Web dla Android OS
- Dr.Web dla Symbian OS
- Dr.Web dla Windows Mobile

Zakres dostawy

- Koperta firmowa
- Certyfikat licencyjny
- Dysk z dystrybuowanym produktem

Więcej szczegółów o Autoryzowanych Centrach Dr.Web – http://partners.drweb.com/service/

Zestawy Dr.Web

W skład zestawów wchodzą produkty Dr.Web do ochrony wszystkich typów obiektów.

WAŻNE! Na zestaw ani na przedłużenie licencji zestawu nie udziela się żadnych zniżek. Aby móc dalej korzystać z zestawu, należy zakupić nową licencję za pełną stawkę. Zniżki na przedłużenie licencji udziela się przy przechodzeniu z zestawu na poszczególne produkty Dr.Web.

Zestaw Dr.Web „Uniwersalny"

Dostępna ochrona kompleksowa klasy enterprise dla małych i średnich przedsiębiorstw.

Niewielkie firmy często nie mogą przeznaczyć znacznych środków na kompleksową ochronę informatyczną. I właśnie z myślą o nich stworzono zestaw Dr.Web „Uniwersalny" – niedrogą ofertę dla organizacji, które mają od 5 do 50 komputerów.

Zestaw „Dr.Web Uniwersalny + Kryptograf" jest dostarczany wraz z licencjami na Atlansys Bastion Pro*.

Produkty	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mail Security Suite	Dr.Web Gateway Security Suite	Dr.Web Mobile Security Suite
Chronione obiekty	Stacje robocze	Serwery	Użytkownicy poczty	Użytkownicy bram pocztowych i internetowych	Urządzenia mobilne
Licencja	Ochrona kompleksowa	Antywirus	Antywirus + Antyspam	Antywirus	Antywirus
Kompletowanie	Od 5 do 50	1	Równa liczbie stacji	Równa liczbie stacji (od 25)	Równa liczbie stacji

Przydatne linki

Zestawy Dr.Web: http://products.drweb.com/bundles/choose/

* Atlansys Bastion Pro opracowała firma „Systemy programowe Atlansys"http://www.atlansys.ru

Zestaw Dr.Web dla szkół

Chronione obiekty	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Licencja	Ochrona kompleksowa + Centrum zarządzania	Antywirus	Antywirus
Kompletowanie	10 – 200	1 – 8	10 – 200

Narzędzia

Narzędzia leczące Dr.Web przeznaczone są do diagnostyki i natychmiastowego leczenia w razie konieczności. Nie zapewniają one stałej ochrony komputera.

Dr.Web CureNet!

Scentralizowane leczenie sieci lokalnych o dowolnej skali, w tym z zainstalowanym antywirusem innego producenta

Potencjalni użytkownicy	Małe, średnie, duże i bardzo duże przedsiębiorstwa, które w sieciach lokalnych mają zainstalowane oprogramowanie antywirusowe innego producenta.
Rozwiązywane zadania	■ Zdalne scentralizowane leczenie stacji roboczych i serwerów Windows. ■ Kontrola jakości ochrony antywirusowej innego producenta.
Właściwości narzędzi	■ Nie wymaga odinstalowania oprogramowania antywirusowego innego producenta przed skanowaniem i leczeniem. ■ Nie wymaga istnienia serwera ani instalacji dodatkowego oprogramowania. ■ Może być używany w sieciach całkowicie odizolowanych od Internetu. ■ Kreator Dr.Web CureNet! można uruchomić z dowolnego zewnętrznego nośnika, w tym z USB.
Opis produktu	http://products.drweb.com/curenet
Wspierane systemy operacyjne	MS Windows 8/2012/7/2008/Vista/2003/XP Professional/2000 (systemy 32- i 64-bitowe).
Czym jest „Mój Dr.Web CureNet!”?	To osobisty gabinet, w którym przez cały okres ważności licencji przechowywany jest indywidualny odsyłacz do pobrania zaktualizowanej wersji oprogramowania. Za pośrednictwem tego gabinetu można również łączyć się z centrum wsparcia technicznego, wysłać podejrzany plik do analizy oraz korzystać z innych usług.
Udzielanie licencji	Licencja na narzędzie udzielana jest na 10, 30 i 365 dni użytkowania w zależności od liczby stacji. Przewiduje się także szczególne licencje serwisowe na 30 i 365 dni. Uprawniają one do świadczenia usług w zakresie leczenia sieci korporacyjnych za pomocą Dr.Web CureNet! firmom z zewnątrz.

Wersja demo	Bez funkcji leczenia.
Wymagania systemowe	Kreator: ■ Dowolny komputer z systemem Windows. ■ Co najmniej 36 MB wolnego miejsca na dysku twardym. ■ Dostęp do Internetu w celu aktualizacji baz wirusów i komponentów Dr.Web CureNet!. ■ Sieć lokalna TCP/IP. Skaner: ■ Co najmniej 17 MB wolnego miejsca na dysku twardym. ■ PC z systemem operacyjnym MS Windows 8/2012/7/2008/Vista/2003/XP Professional/2000 (systemy 32- i 64-bitowe).

Dr.Web CureIt!

Natychmiastowe leczenie PC i serwerów z systemem Windows, w tym z zainstalowanym oprogramowaniem antywirusowym innego producenta

Potencjalni użytkownicy	Małe i średnie przedsiębiorstwa, które w swoich komputerach i serwerach mają zainstalowany program antywirusowy innego producenta.
Rozwiązywane zadania	■ Natychmiastowe leczenie stacji roboczych i serwerów Windows. ■ Kontrola jakości ochrony antywirusowej innego producenta.
Właściwości narzędzi	■ Nie wymaga instalacji, jest kompatybilne z każdym antywirusem, co oznacza, że na czas skanowania nie trzeba wyłączać zainstalowanego programu antywirusowego innego producenta. ■ Podwyższona samoochrona i wzmocniony tryb skutecznego przeciwdziałania blokerom Windows. ■ Aktualizacje raz lub kilka razy na godzinę. ■ Narzędzie można uruchomić z dowolnego zewnętrznego nośnika, w tym z USB.
Opis produktu	http://free.drweb.com/cureit
Wspierane systemy operacyjne	MS Windows 2000/XP/2003/Vista/2008/7 (systemy 32- i 64-bitowe).
Udzielanie licencji	Licencja na narzędzie udzielana jest na10, 30 i 365 dni użytkowania w zależności od liczby stacji. Przewiduje się także szczególne licencje serwisowe na 30 i 365 dni. Uprawniają one do świadczenia usług w zakresie leczenia komputerów i serwerów za pomocą Dr.Web CureIt! firmom z zewnątrz.
Szczególne cechy udzielania licencji	Narzędzie jest bezpłatne do leczenia prywatnego komputera domowego.
Wersja demo	Niedostępna.

Zestawy programowo-sprzętowe Dr.Web Office Shield

Wysokowydajne i niezawodne serwery dla zapewnienia kompleksowej, scentralizowanej ochrony stacji roboczych i serwerów plików Windows oraz ruchu pocztowego i internetowego

Zalety

- Niedroga ochrona sieci korporacyjnej za pomocą rozwiązania klasy enterprise.
- Możliwość wykorzystania rozwiązania w przypadku braku wysoko wykwalifikowanych specjalistów („zainstalowane i zapomniane").
- Ograniczenie strat czasu pracy, przestojów urządzeń i personelu dzięki zmniejszeniu liczby incydentów wirusowych i wysokiej odporności urządzeń na ataki z zewnątrz.
- Istotne obniżenie kosztów ruchu sieciowego i możliwość monitorowania działań pracowników w Internecie.
- Oszczędność czasu roboczego administratora systemowego dzięki prostocie instalacji.

Dr.Web Office Shield można wykorzystywać w postaci:

- serwera strefy zdemilitaryzowanej – urządzenia maksymalnie odizolowanego od sieci wewnętrznej, odpowiadającego za ochronę antywirusową i antyspamową przedsiębiorstwa;
- serwera proxy (bramy dostępu użytkowników wewnętrznej sieci intranetowej do zasobów Internetu), przeznaczonego do zabezpieczania ruchu pocztowego i internetowego przed wirusami oraz różnorodnymi obiektami złośliwymi i spamem. Wykorzystanie Dr.Web Office Shield w postaci bramy w znacznym stopniu obniża koszty firm, związane z zapewnieniem bezpieczeństwa dostępu do sieci i pozwala istotnie zmniejszyć ruch sieciowy;
- wewnętrznego serwera sieci lokalnej, zapewniającego scentralizowaną ochronę stacji roboczych i serwerów plików Windows.

Dr.Web Office Shield można zainstalować w istniejącej sieci lub wykorzystać w formie bazy do stworzenia nowej sieci – jest to ważna cecha tego zestawu programowo-sprzętowego. Serwisy DHCP i DNS pozwolą wykonać tę pracę przy minimalnym wysiłku.

W skład zestawu Dr.Web Office Shield wchodzą:

- Dr.Web Desktop Security Suite – scentralizowana ochrona stacji roboczych i serwerów plików Windows;
- Dr.Web dla bram internetowych UNIX – ochrona dostępu użytkowników wewnętrznej sieci intranetowej do zasobów Internetu;
- Dr.Web dla bram pocztowych UNIX – ochrona antywirusowa i antyspamowa ruchu pocztowego;
- Korporacyjny ekran międzysieciowy;
- Serwer VPN;
- Serwer DHCPSDNS;
- Punkt dostępu Wi-Fi.

Rodzaje dostawy

NEO

Chronione obiekty

- ruch pocztowy;
- ruch internetowy;

Zalecana liczba użytkowników: od 10 do 150.

Chronione obiekty

- stacje robocze Windows;
- serwery plików Windows;
- ruch pocztowy;
- ruch internetowy;

Zalecana liczba użytkowników: od 10 do 50.

TWISTER

Chronione obiekty

- stacje robocze Windows;
- serwery plików Windows;
- ruch pocztowy;
- ruch internetowy;

Zalecana liczba użytkowników: od 50 do 250.

Chronione obiekty

- ruch pocztowy;
- ruch internetowy;

Zalecana liczba użytkowników: od 50 do 250.

Udzielanie licencji

- Nielimitowana licencja.
- Licencja według liczby chronionych obiektów: stacji roboczych, użytkowników poczty i bram.
- Zastosowanie mają wszystkie istniejące w chwili zakupu zniżki, przewidziane dla produktów Dr.Web (nie dotyczy nielimitowanej licencji).

Warunki udzielania licencji bez limitu

Urządzenie NEO	Urządzenie TWISTER
■ Centrum zarządzania ■ Dr.Web Desktop Security Suite, Kompleksowa ochrona (50 PCs) ■ Dr.Web Server Security Suite (5 serwerów) ■ Dr.Web Mail Security Suite, Antywirus + Antyspam + SMTP proxy (50 użytkowników) ■ Dr.Web Gateway Security Suite, Antywirus (50 użytkowników)	■ Centrum zarządzania ■ Dr.Web Desktop Security Suite, Kompleksowa ochrona (250 PCs) ■ Dr.Web Server Security Suite (25 serwerów) ■ Dr.Web Mail Security Suite, Antywirus + Antyspam + SMTP proxy (250 użytkowników) ■ Dr.Web Gateway Security Suite, Antywirus (250 użytkowników)

- Licencja jest warunkowo bez limitu, ponieważ jej parametry są ograniczone parametrami sieci aparatowej urządzeń.
- Licencja jest przeznaczona tylko dla nowych klientów.
- Licencja jest dostarczana tylko pod warunkiem jednoczesnego zakupu urządzenia (sprzętu).
- Koszt tej licencji nie obejmuje rabatów na przedłużenie, rabatów dla placówek edukacyjnych i medycznych.
- Licencja bez limitu jest udzielana tylko na 1 rok.
- Przedłużenie licencji bez limitu następuje według liczby niezbędnych klientowi obiektów do ochrony.
- Do licencji bez limitu nie dokonuje się dodatkowych zakupów.

Dr.Web LiveDemo

Serwis zdalnego testowania online Dr.Web LiveDemo pozwala jeszcze przed nabyciem zestawu programowo-sprzętowego wypróbować wybraną konfigurację w wirtualnej sieci lokalnej na serwerze firmy „Doktor Web".

Rozwiązania

Dr.Web Security Suite dla Unix Appliance

Modułowa grupa rozwiązań, przeznaczonych do integracji z zestawami programowo-sprzętowymi, zbudowanymi na bazie systemów operacyjnych Unix (Linux/FreeBSD/Solaris (x86)).

Rozwiązania spełniają funkcje korporacyjnej bramy internetowej – serwera proxy, używanego do organizacji dostępu użytkowników wewnętrznej sieci intranet do zasobów sieci Internet.

	Dr.Web Mail Security Suite dla Unix Appliance	**Dr.Web Gateway Security Suite dla Unix Appliance**
Funkcja kluczowa	Filtracja wiadomości pocztowych pod kątem wirusów i spamu.	Filtracja ruchu sieciowego HTTP i FTP pod kątem wirusów
Wersje licencji	Antywirus Antywirus + Antyspam	Antywirus

Rodzaje licencji

- Pod względem liczby chronionych użytkowników (jest ona nieograniczona).
- Licencja serwerowa – do skanowania nieograniczonej ilości korespondencji / ruchu sieciowego na jednym serwerze, z maksymalnie 3000 chronionych użytkowników.

Udzielanie licencji SDK

SDK jest rozpowszechniane bezpłatnie w składzie produktu. Użytkownicy z zewnątrz mogą dowolnie opracowywać i rozpowszechniać dodatki na bazie SDK na warunkach niekomercyjnych. Do rozpowszechniania komercyjnego należy przejść proces certyfikacji.

Dr.Web ATM Shield

Rozwiązanie do scentralizowanej ochrony w czasie rzeczywistym wbudowanych systemów komputerowych (bankomatów, multikiosków, sieci kasowych itp.).

Za podstawę stworzenia specjalnego rozwiązania do ochrony wbudowanych systemów posłużył produkt biznesowy firmy „Doctor Web" – Dr.Web Desktop Security Suite z możliwością scentralizowanego zarządzania.

Zalety

- Łatwość integracji w sieci bankomatów i urządzeń kasowych i w rezultacie istotne skrócenie czasu ich obsługi;
- Scentralizowane zarządzanie wszystkimi komponentami antywirusowej ochrony wbudowanych systemów;
- Łatwa skalowalność, zapewniająca możliwość wykorzystywania w sieciach o nieograniczonej ilości węzłów (dzięki hierarchicznej strukturze sieci antywirusowej);
- Platformowość krzyżowa oprogramowania antywirusowego – możliwość instalacji serwera zarówno na systemie operacyjnym Microsoft Windows, jak i Unix;
- Praca w sieciach, opartych na połączeniu TCP/IP, IPX, NetBIOS;
- Możliwość wyboru typu SUBD serwera ochrony;
- Minimalny ruch sieciowy, oparty na specjalnie opracowanym protokole wymiany informacji w sieciach, zbudowanych na bazie protokołów TCP/IP, IPX/SPX i NetBIOS z możliwością zastosowania specjalnych algorytmów kompresji ruchu sieciowego;

- Oszczędność ruchu w sieci zapewnia specjalny zoptymalizowany protokół, wspierający kompresję danych między klientem a serwerem;
- Możliwość szyfrowania danych przy wymianie między różnymi komponentami systemu;
- Monitoring stanu wszystkich chronionych węzłów sieci;
- Scentralizowane zbieranie statystyki incydentów wirusowych;
- Rezerwowe kopiowanie krytycznych danych serwera ochrony sieci;
- Przejrzystość pracy – dziennik audytowy rejestrujący czynności administratorów pozwala na śledzenie wszystkich kroków, dotyczących instalacji i konfiguracji systemu.

Udzielanie licencji

Dr.Web ATM Shield jest licencjonowany według liczby chronionych wbudowanych urządzeń podłączanych do serwera antywirusowego. Licencje na Centrum zarządzania udzielane są bezpłatnie. Przewiduje się licencje na 1, 2 i 3 lata.

Serwisy

Software as a service (SAAS) – szeroko rozpowszechniony poza granicami Rosji model udostępniania oprogramowania jako usługi.

W rosyjskiej branży antywirusowej do roku 2007 ten model nie był wykorzystywany. Było to związane po prostu z brakiem krajowych rozwiązań podobnej klasy. Wszystko zmieniło się w maju 2007 roku, kiedy to rosyjska firma „Doctor Web" wydała własny serwis internetowy Dr.Web AV-Desk. Na rynku usług IT w Rosji pojawił się nowy segment – segment usług ochrony antywirusowej. Pierwszą wśród nich stała się usługa „Antywirus Dr.Web".

Serwis internetowy Dr.Web AV-Desk

Co to jest Dr.Web AV-Desk?	Dr.Web AV-Desk – to serwis internetowy do udostępniania zestawu usług online, w zakresie ochrony informacyjnej PC i serwerów, nieograniczonej liczbie klientów – użytkowników domowych i biznesowych. Dr.Web AV-Desk – to oprogramowanie pozwalające w sposób scentralizowany zarządzać procesem świadczenia usługi „Antywirus Dr.Web" Dr.Web AV-Desk – to model biznesu VAD, za pomocą którego można łatwo pozyskiwać nowych klientów i zwiększać dochody.
Dla kogo jest przeznaczony serwis Dr.Web AV-Desk?	Dla dostawców Internetu i wszelkich innych firm, działających w dziedzinie technologii informacyjnych.
Dla kogo jest przeznaczona usługa „Antywirus Dr.Web"?	Dla osób fizycznych i prawnych – klientów dostawców usługi.
Jakie usługi może świadczyć dostawca, korzystając z Dr.Web AV-Desk?	Usługi w zakresie ochrony informacyjnej PC klientów przed wirusami, spamem i wszelkiego rodzaju złośliwymi programami. Są one świadczone w postaci abonamentu na dowolny okres, wygodny dla użytkownika. Za prawo korzystania z funkcji ochronnych oprogramowania Dr.Web pobiera się opłatę abonamentową.

Oprogramowanie Dr.Web AV-Desk	Zestaw programowy do scentralizowanego zarządzania procesem świadczenia usług w zakresie ochrony informacyjnej PC klientów dostawców usługi.
Udzielanie licencji Dr.Web AV-Desk	Serwis Dr.Web AV-Desk jest udostępniany dostawcy usługi bezpłatnie. Natomiast licencja na usługę „Antywirus Dr.Web" jest udzielana według liczby abonentów, podłączonych do serwisu w okresie sprawozdawczym (miesiąc), dla których nie upłynął okres ważności usługi.

Jak to działa?

Dostawca usługi	Klienci usługi
■ Organizuje subskrypcję (abonament) usługi „Antywirus Dr.Web" poprzez Centrum Zarządzania Subskrypcją. ■ Zapewnia klientom usługi najnowsze aktualizacje baz wirusów i modułów programowych Dr.Web. ■ Udziela wsparcia technicznego (opcjonalnie). ■ Śledzi stan sieci antywirusowej i zbiera informacje statystyczne o infekcjach wirusowych. ■ Świadczy usługi dodatkowe. ■ Pobiera od klientów opłatę za korzystanie z usługi.	■ Wykupują subskrypcję (abonament) w Centrum Zarządzania Subskrypcją. ■ Dokonują instalacji oprogramowania Dr.Web. ■ Samodzielnie sterują parametrami abonamentu. ■ Uiszczają opłatę abonamentową dostawcy usługi.

Dr.Web AV-Desk to wielowariantowy model biznesu. Dostawcami usługi „Antywirus Dr.Web" mogą zostać dostawcy Internetu lub wszelkie inne firmy, działające w sferze technologii informacyjnych.

	Dystrybutor usługi „Antywirus Dr.Web"	Dostawca usługi „Antywirus Dr.Web"	Agregator serwisu Dr.Web AV–Desk
Podstawowa działalność	Firma realizuje abonament na usługę „Antywirus Dr.Web" dla użytkowników końcowych poprzez wbudowane w swoją stronę Centrum Zarządzania Subskrypcją.	Firma wdraża serwis Dr.Web AV-Desk i świadczy usługę „Antywirus Dr.Web" użytkownikom końcowym.	Firma posiada własny serwer, na który wdraża serwis Dr.Web AV-Desk, tworzy własną sieć dystrybutorów usługi i udziela im sublicencji na Centrum Zarządzania Subskrypcją. Agregator nie ma prawa realizacji usługi dla użytkowników końcowych.

Bardziej szczegółowe informacje o Dr.Web AV-Desk i usłudze „Antywirus Dr.Web" są udzielane partnerom na żądanie.

Polityka rabatów

Współczynniki rabatów są stosowane do ceny licencji na 1 rok (zgodnie z cennikiem).

Jeśli użytkownik ma prawo do kilku rodzajów rabatów, to rabaty te nie sumują się, lecz jest udzielany najwyższy z nich (z wyjątkiem rabatów dla dostawców internetowych).

Obowiązywanie rabatów obejmuje tylko rozwiązania cenowe. Rozszerzenie obowiązywania rabatów na rozwiązania pozacenowe należy uzgadniać z menedżerami firmy „Doctor Web".

Rabaty ze względu na liczbę licencjonowanych produktów

Rabaty ze względu na liczbę licencjonowanych produktów (typów licencjonowanych obiektów) są naliczane od sumy cen licencji bazowych i cen licencji dodatkowych komponentów – osobno dla każdego produktu. Te rabaty są stosowane automatycznie w kalkulatorze.

Liczba licencjonowanych produktów	Rabat
4	30%
3	25%
2	20%

Ograniczenia

Rabatów nie stosuje się, jeśli:

- liczba serwerów wynosi mniej niż 10% liczby stacji, użytkowników poczty lub bram;
- liczba użytkowników poczty lub bram jest mniejsza od liczby stacji;
- liczba użytkowników bram jest mniejsza od liczby użytkowników poczty i odwrotnie.

Tabela rabatów

Typ klienta	Podstawa rabatu	Nowa licencja			Przedłużenie			Migracja*		
		1 rok	2 lata	3 lata	1 rok	2 lata	3 lata	1 rok	2 lata	3 lata
Kategorie bez zniżek	Dla rabatu na przedłużenie – plik klucza lub numer seryjny Dr.Web na okres co najmniej 6 miesięcy na analogiczny produkt Dr.Web.	–	1,6	2,17	0,6	1,17	1,72	0,5	1	1,5
	Dla rabatu na migrację – oryginał licencji/plik klucza/ pismo potwierdzające zakup elektronicznej wersji antywirusa innego producenta.									
Uczelnie, biblioteki, muzea i placówki służby zdrowia	Kopia dokumentu wystawionego przez odpowiedni organ, poświadczającego że dana jednostka ma prawo do działalności edukacyjnej czy ochrony zdrowia, oraz wypełniona ankieta.	0,5	0,85	1,2	0,35	0,7	1,05			

Przedłużenie

1. Można przedłużyć z rabatem zarówno licencję obowiązującą, jak i po upływie okresu obowiązywania. Nie ma terminu przedawnienia dla przedłużenia licencji Dr.Web.
2. Można przedłużyć z rabatem licencję na analogiczny produkt lub rozwiązanie Dr.Web. Okres obowiązywania takiej licencji powinien wynosić co najmniej 3 miesiące.
3. Rabatu na przedłużenie udziela się pod warunkiem nabycia licencji na 1, 2 lub 3 lata na analogiczny produkt lub rozwiązanie Dr.Web.
4. Licencja przedłużenia z rabatem jest udzielana na liczbę chronionych obiektów, nieprzekraczającą liczby chronionych obiektów podanej w poprzedniej (przedłużanej) licencji.

5. Podstawą do uzyskania rabatu na przedłużenie jest plik klucza lub numer seryjny Dr.Web, który może być przedłużony tylko jeden raz.
6. Aby uzyskać rabat na przedłużenie, użytkownik powinien przedstawić sprzedawcy numer seryjny lub plik klucza (w tym OEM).

„Przechodź na zielonym!"

Program migracji rabatowej dla Dr.Web dla użytkowników antywirusów innych producentów.

1. Niniejsza oferta specjalna obejmuje tylko produkty Dr.Web. Komplety, narzędzia, zestawy programowosprzętowe, serwisy i rozwiązania nie biorą udziału w programie migracji rabatowej.
2. Rabatu nie udziela się osobom prywatnym. Mogą go uzyskać tylko organizacje i firmy tylko jeden raz.
3. Rabat przy przechodzeniu nie jest udzielany użytkownikom licencji OEM.
4. Przy przechodzeniu na roczną licencję Dr.Web jest udzielany rabat 50%. Przy przechodzeniu na dwu- i trzyletnie licencje używa się do obliczenia kosztu odpowiednio współczynnika 1 lub 1,5, który mnoży się przez cenę rocznej licencji Dr.Web.
5. Rabat przy przechodzeniu z innego antywirusa jest udzielany tylko na analogiczny produkt z rodziny Dr.Web (według typu i liczby chronionych obiektów).
6. Aby otrzymać rabat na migrację, użytkownik powinien przedstawić oryginał licencji, plik klucza lub pismo potwierdzające zakup elektronicznej wersji antywirusa innego producenta z informacją o rejestracji.
7. Rabat jest udzielany użytkownikom zarówno licencji obowiązujących, jak i po upływie ich obowiązywania pod warunkiem, że od chwili upływu okresu obowiązywania licencji do zwrócenia się do partnera firmy „Doctor Web" minęło nie więcej niż 30 dni.
8. Jeśli okres obowiązywania licencji na antywirus innego producenta nie upłynął do dnia opłaty licencji na migrację, to pozostały czas dodaje się bezpłatnie do okresu obowiązywania nowej licencji.
9. Dalsze przedłużanie licencji migracyjnej odbywa się ze zwykłym rabatem na przedłużenie.
10. Rabaty migracyjne nie sumują się z żadnymi innymi rabatami.

Ogólne warunki sprzedaży

1. Partnerzy mają obowiązek sprzedawać programy Dr.Web końcowym użytkownikom w ścisłej zgodności z zestawami i zgodnie z zalecanymi cenami, ustalonymi w cenniku.
2. Dla wszystkich produktów Dr.Web w standardowych zestawach i w cenach cennikowych koszt aktualizacji modułów programowych i baz wirusów oraz bazowe wsparcie techniczne online na stronie http://support.drweb.com są wliczone w koszt licencji na cały okres jej obowiązywania.
3. Przy zamawianiu licencji w pudełku firmowym cena zwiększa się o wartość zestawu mediowego.
4. Jeśli klient potrzebuje rozwiązania do ochrony większej liczby obiektów, niż jest podana w cenniku, partner ma obowiązek zażądać cen od firmy „Doctor Web" i przekazać online pod adresem https://pa.drweb.com/support następujące dane klienta:
   - nazwa firmy;
   - adres;
   - e-mail;
   - telefon pracownika serwisu technicznego, odpowiedzialnego za ochronę antywirusową;
   - dane kontaktowe działu wsparcia technicznego.

Wszystkie rodzaje rabatów przy zakupie takich rozwiązań są udzielane użytkownikowi końcowemu tylko po uzgodnieniu z firmą „Doctor Web".

5. Ceny rozwiązań niewymienionych w cenniku, są ustalane w umowie licencyjnej, która jest zawierana przez firmę „Doctor Web" bezpośrednio z dostawcą takich rozwiązań dla użytkownika końcowego.

Rozszerzenie licencji

Jeśli użytkownik chce zmienić licencję bazową (np. z Antywirusa na Ochronę kompleksową) lub dodać do istniejącej licencji bazowej dodatkowe komponenty (kryptograf, antyspam lub SMTP proxy), proponuje się rabatowe przejście na potrzebną licencję w cenie licencji przedłużenia. Od chwili opłaty licencji przedłużenia i aktywacji nowego numeru seryjnego użytkownik zyskuje możliwość korzystania ze wszystkich dodatkowych komponentów, a okresy obowiązywania poprzedniej i nowej licencji sumują się. Niniejsze warunki rabatowego rozszerzenia licencji obowiązują także dla licencji, dla których upłynął okres obowiązywania.

Kreator przedłużenia: http://products.drweb.com/renew/

Dodatkowy zakup

1. W przypadku zwiększenia liczby chronionych obiektów w trakcie okresu obowiązywania licencji koszt dodatkowo kupowanych licencji jest wyliczany według bieżącego cennika bez rabatu, proporcjonalnie do pozostałego okresu obowiązywania licencji.
2. Pozostały okres obowiązywania licencji jest wyliczany na podstawie liczby miesięcy, pozostałych do upływu okresu obowiązywania wcześniej nabytej licencji (przy tym niepełny miesiąc zaokrągla się do 1 miesiąca).
3. Minimalny możliwy okres obowiązywania licencji przy dodatkowym zakupie – 6 miesięcy. Maksymalny – 30 miesięcy. W przeciwnym razie rozszerzenie licencji dokonuje się na zasadach dodatkowego zakupu + przedłużenia.
4. Koszt dodatkowo kupowanych licencji wylicza się na podstawie zakresu łącznej liczby chronionych obiektów.

Dodatkowy zakup + przedłużenie

Przy jednoczesnym przedłużeniu i dodatkowym zakupie koszt DODATKOWO KUPOWANYCH licencji wylicza się na podstawie ceny zakresu łącznej liczby nabywanych licencji (przedłużanych + dodatkowo kupowanych). Koszt PRZEDŁUŻANYCH licencji wylicza się na podstawie ceny zakresu łącznej liczby PRZEDŁUŻANYCH licencji.

Kreator dodatkowego zakupu: http://promotions.drweb.com/upgrade

Kody produktów, zestawów, narzędzi i zestawów programowo-sprzętowych Dr.Web

Zasady tworzenia kodów

1. Kod zawsze składa się z 5 grup.
2. Każda grupa kodu jest oddzielona od drugiej grupy łącznikiem.
3. Kod licencji dla kategorii „Produkty" jest tworzony dla każdego produktu komercyjnego Dr.Web osobno (zob. rozdział „Linia produktów Dr.Web Security Suite").
4. Kody zestawów programowo-sprzętowych Dr.Web Office Shield składają się z dwóch kodów:
   - kodu urządzenia,
   - kodu licencji.
5. Kody produktów ogólnodostępnych, kart-zdrapek i pakietów medialnych oraz kody urządzeń PAK Dr.Web Office Shield są ustalone w cenniku.
6. W kodzie licencji „dodatkowego zakupu" podaje się 2 okresy obowiązywania: ogólny okres obowiązywania dodatkowo kupionej licencji i – po dwukropku – pozostały okres obowiązywania załączonego (działającego) klucza.
7. W kodzie licencji „dodatkowego zakupu + przedłużenia" podaje się 2 okresy obowiązywania: ogólny okres obowiązywania dodatkowo kupionej i przedłużanej licencji i – po dwukropku – pozostały okres obowiązywania załączonego (działającego) klucza.
8. W kodzie licencji „dodatkowego zakupu" podaje się 2 liczby chronionych obiektów: ogólną liczbę licencji z uwzględnieniem dodatkowego zakupu i – po dwukropku – liczbę obiektów obowiązującej (załączonej) licencji.
9. W kodzie licencji „dodatkowego zakupu + przedłużenia" podaje się 2 liczby chronionych obiektów: ogólną liczbę licencji z uwzględnieniem dodatkowego zakupu i – po dwukropku – liczbę obiektów obowiązującej (przedłużanej) licencji.

Tabela porównawcza symboli kodów

Grupa 1			Grupa 2		Grupa 3	Grupa 4	Grupa 5	
Kompletowanie	**Kategoria produktów**	**Chronione obiekty**	**Licencja bazowa**	**Dodatkowe komponenty**	**Okres obowiązywania licencji**	**Liczba chronionych obiektów**	**Typ licencji**	**Typ użytkownika**
L Licencja elektroniczna pobierana ze strony internetowej	**B** produkt dla firm **H** produkt dla domu	**G** użytkownicy bramy	**A** Antywirus	**A** Antyspam	**XXM** gdzie XX to liczba miesięcy	dowolna liczba	**A** nowa licencja	**1** zniżka dla edukacji, służby zdrowia, bibliotek, muzeów
B produkt w pudełku kartonowym **A** promocyjny produkt w pudełku kartonowym	**X** licencja dostarczana w składzie Dr.Web Office Shield	**M** urządzenia mobilne	**B** Ochrona kompleksowa	**C** Centrum zarządzania	**XXXD** gdzie XXX to liczba dni	**UL** unlimited (dla licencji nieograniczonej)	**B** przedłużenie **C** dokupienie	**2** promocja **3** bez rabatu
C karta zdrapka	**Y** Narzędzia do leczenia	**P** użytkownicy poczty	* – licencje dla kilku produktów (stosowane dla Zestawów).	**K** bez dodatkowych komponentów			**D** przedłużenie z dokupieniem	**4** migracja
D Produkt dostarczany w pudełku DVD	**Z** zestaw	**S** serwery		**R** Kryptograf			**F** – Licencja OEM	**5** licencja NFR dla partnera
K program dostarczany w pakiecie licencyjnym		**W** stacje robocze		**S** SMTP proxy			**G** – licencja serwisowa	**6** licencja (demo) NFR dla klienta
M program na dysku firmowym (w tym OEM)		**Z** wszystkie obiekty						**7** działania marketingowe
N produkt dostarczany w certyfikowanym pakiecie licencyjnym								**8** akcje charytatywne
P produkt dostarczany w pakiecie OEM								**9** podział klucza
								10 łączenie kluczy
								11 zmiana klucza

Przykłady

Przykłady kodów licencji dla kategorii «Produkty»

1.	Zamawiającej placówce edukacyjnej potrzebna jest ochrona 200 PC z Centrum zarządzania, Ochrona kompleksowa + zapora, na 12 miesięcy, licencja elektroniczna. Dr.WEB nabywany po raz pierwszy.	**LBW-BRC-12M-200-A1**
2.	Zamawiająca placówka edukacyjna posiada obowiązującą licencję do ochrony 200 PC z Centrum zarządzania, Ochroną kompleksową i zaporą, na 12 miesięcy, licencja elektroniczna, do upływu okresu obowiązywania której pozostało 6 miesięcy. Powinna dokupić ochronę dla 10 stacji.	**LBW-BRC-6M:6M-210:200-C1**
3.	Zamawiająca placówka edukacyjna posiada licencję z przykładu 2, do upływu okresu obowiązywania której pozostało 7 miesięcy. Musi dokupić ochronę dla 10 stacji i jednocześnie przedłużyć licencję o kolejne 2 lata.	**LBW-BRC-31M:7M-210:200-D1**

Przykłady kodów licencji dla kategorii «Zestawy»

1.	Zamawiający potrzebuje zestawu Dr.Web „Uniwersalny", ochrony 50 PC z Centrum zarządzania, Ochrony kompleksowej, na 12 miesięcy, licencja elektroniczna.	**LZZ-*CR-12M-50-A3**
2.	Zamawiający potrzebuje zestawu Dr.Web „Uniwersalny", ochrony 50 PC z Centrum zarządzania, Ochrony kompleksowej, na 12 miesięcy, licencja elektroniczna.	**LZZ-*C-12M-50-A3**
3.	Zamawiająca placówka edukacyjna (szkoła) potrzebuje ochrony dla 100 PC.	**LZZ-*C-12M-100-A1**

Przykłady kodów licencji dla kategorii „Narzędzia"

1.	Zamawiający musi przeprowadzić leczenie 100 PC w ciągu 10 dni. PC są połączone w sieć korporacyjną.	**LYW-AC-10D-100-A3**
2.	Zamawiający musi przeprowadzić leczenie 10 PC w ciągu 30 dni. PC nie są połączone w sieć korporacyjną.	**LYW-AK-30D-10-A3**

Przykłady kodów licencji dla kategorii „PAK Dr.Web Office Shield"

Tworzy się tyle kodów, na ile produktów Dr.Web udziela się licencji

1.	Zamawiający – placówka oświatowa potrzebuje ochrony 25 użytkowników poczty (AB + AC + SMTP proxy) i 50 użytkowników bramy internetowej.	**LXP-AASC-12M-25-A1** **LXG-AK-12M-50-A1**
2.	Zamawiający potrzebuje Ochrony kompleksowej 150 PC, 1 serwera Windows, 100 użytkowników poczty (tylko antywirus) i 50 użytkowników bramy internetowej.	**LXW-BC-12M-150-A3** **LXS-AC-12M-1-A3** **LXP-AC-12M-100-A3** **LXG-AC-12M-50-A3**
3.	Zamawiający posiada licencję z przykładu 2, do upływu okresu obowią-zywania której zostało 7 miesięcy. Musi dokupić ochronę dla jeszcze 20 PC i przedłużyć licencję o 1 rok.	**LXW-BC-19M:7M-170:150-D3** **LXS-AC-19M-1-B3** **LXP-AC-19M-100-B3** **LXG-AK-19M-50-B3**

Przykłady kodów dla produktów OEM

1.	Partner kupuje 500 kart OEM w pakietach medialnych.	**PHW-B-6M-1-F3**
2.	Partner kupuje 500 licencji OEM, dostarczanych na dyskach	**MHW-B-6M-1-F3**

Kontakty

Rosja

„Doctor Web" Sp. z o.o.

Rosja, 1251 24, Moskwa, 3. ulica Jamskiego Pola, bl. 2, korp. 12a
Telefon: +7 (495) 789-45-87 (wielokanałowy)
Faks: + 7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com

Niemcy

Doctor Web Deutschland GmbH

Niemcy, 63457 Hanau, Rodenbacher Chaussee 6
Telefon: +49 (6181) 9060-1210
Faks: +49 (6181) 9060-1212
www.drweb-av.de

Kazachstan

„Doctor Web – Azja Centralna" Sp. z o.o.

Republika Kazachstanu, 050009, Ałmaty
ul. Szewczenko / róg ul. Radostowca, 165b/72g, biuro 910
Telefon: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32
www.drweb.kz

Ukraina

Centrum Wsparcia Technicznego „Doctor Web"

Ukraina, 01001, Kijów, ul. Kostielnaja 4, lok. 3
Telefon / Faks: +38 (044) 238-24-35, +38 (044) 279-77-70
www.drweb.ua

Francja

Doctor Web France

333 b Avenue de Colmar, 67100 STRASBOURG
Telefon: +33 (0) 3-90-40-40-20
Faks: +33 (0) 3-90-40-40-21
www.drweb.fr

Japonia

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F
1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005
Telefon: +81(0) 44-201-771 1
www.drweb.co.jp