Dr.WEB®
seit 1992

Defend what you create

Produktpalette Dr.Web Security Suite

Lizenzierungsanleitung

Inhaltsverzeichnis

© Doctor Web, 2016

© Doctor Web, 2016

Über Doctor Web

Doctor Web ist ein führender russischer Anbieter hauseigener IT-Sicherheitslösungen.

Dr.Web Antivirensoftware wird seit 1992 permanent weiterentwickelt und weist hervorragende Ergebnisse bei der Erkennung und Beseitigung von Malware auf. Mit der Gründung des Unternehmens im Jahre 2003 konnte man ein rapides Verkaufswachstum sowohl in Russland als auch in anderen Ländern erreichen.

Heute ist Doctor Web ein erfolgreiches und massiv wachsendes Unternehmen, das eine führende Rolle am Markt für IT-Sicherheit spielt. Das Unternehmen verfügt über die hauseigene Antiviren-Engine, unterhält ein Virenlabor, einen globalen Virenüberwachungsdienst und bietet seinen Kunden einen kostenlosen technischen Support an.

Das Ziel der Mitarbeiter ist es, Sicherheitslösungen zu entwickeln, die sämtlichen modernen Anforderungen entsprechen. Die Entwicklung neuer technologischer Lösungen, die Anwendern bei der Bekämpfung von beliebigen Virenbedrohungen helfen sollen, spielt eine wichtige Rolle. Die Produktpalette von Doctor Web umfasst eine große Zahl von Betriebssystemen und kompatiblen Anwendungen.

Bei der Distribution von Dr.Web Antivirenprodukten greift das Unternehmen auf ein höchstprofessionelles Partnernetzwerk zurück.

Zu den Kunden von Doctor Web gehören Privatanwender aus verschiedenen Regionen der Welt, namhafte russische und international agierende, börsennotierte Großunternehmen, Banken und öffentliche Einrichtungen. Zahlreiche Zertifikate und Auszeichnungen zeugen von einem hohen Maß an Vertrauen in Dr.Web Antivirensoftware.

Dr.Web Technologien

Dr.Web Antivirus ist eine Familie von Antivirenprogrammen, die von russischen Programmierern unter Leitung von Igor Danilov entwickelt wurden.

Doctor Web ist einer der wenigen Anbieter weltweit, der über hauseigene Technologien zur Erkennung und Beseitigung von Malware verfügt. Das Unternehmen unterhält einen Virenüberwachungsdienst und ein analytisches Virenlabor. So können die Sicherheitsspezialisten auf neue Virenbedrohungen sekundenschnell reagieren und eine Problemlösung für Kunden in kürzester Zeit anbieten.

Dr.Web zeichnet sich durch seine modulare Architektur aus. Alle Produkte und Lösungen verfügen über eine Antiviren-Engine und verwenden das Update-System für Virendatenbanken und den global agierenden technischen Support. Dr.Web Technologien bieten einen zuverlässigen Virenschutz sowohl für große Unternehmensnetzwerke als auch für Ihren Home-PC.

Außer Viren und Malware kann Dr.Web unerwünschte Programme (Adware, Dialer, Scherzprogramme, Riskware), Spam-Mails und unerwünschte Mails (Fisihing-, Farming-, Scam- und Bounce-Mails) entdecken und löschen.

Ein wichtiger Gradmesser für die Qualität eines Antivirenprogramms ist nicht nur seine Fähigkeit, Viren & Co. zu entdecken, sondern diese auch zu desinfizieren und infizierte Dateien nicht nur zu löschen, sondern diese auch zu reparieren.

© Doctor Web, 2016

Virendesinfektion

- Dr.Web läuft auf einem bereits infizierten PC und verfügt über eine ausschließliche Virenresistenz
- Doctor Web ist Branchenführer bei der effektiven Desinfektion aktiver Viren
- Technologien für die Bearbeitung von Prozessen im Hauptspeicher und hervorragende Möglichkeiten bei der Neutralisierung aktiver Vireninfektionen ermöglichen die Installation von Dr.Web auf einem infizierten PC (ohne vorherige Desinfektion)
- Starten der Prüfung auf einem infizierten PC, u.a. vom Wechseldatenträger, ohne Installation im System (z.B. vom USB-Stick)

Selbstschutz

Das Selbstschutz-Modul **Dr.Web SelfPROtect** sorgt für eine hohe Resistenz des Programms gegenüber Evasions-Techniken.

- **Dr.Web SelfPROtect** ist als Treiber realisiert und läuft auf der niedrigsten Systemebene. Das Entladen und Abbrechen des Moduls vor dem Neustart des Systems ist nicht möglich.
- **Dr.Web SelfPROtect** schränkt den Zugriff böswilliger Objekte auf das Netzwerk, Dateien und Verzeichnisse, einige Registerzweige und Wechseldatenträger auf Ebene des Systemtreibers ein und schützt gegen Evasions-Techniken
- Im Vergleich zu Konkurrenzprogrammen, die den Windows-Kernel modifizieren (Vektortabellen vorschieben, nicht dokumentierte Funktionen verwenden usw.), was ernsthafte Probleme für das Betriebssystem bewirken kann und neue Sicherheitslücken öffnet, läuft **Dr.Web SelfPROtect** vollständig autonom
- Automatisches Wiederherstellen eigener Module

Einzigartige Möglichkeiten der Engine

- Prüfung von Archiven mit beliebiger Rekursionstiefe
- Entdeckung gepackter, böswilliger Objekte mit hoher Genauigkeit und Analyse einzelner Komponenten auf versteckte Bedrohungen
- Doctor Web ist Branchenführer bei der Erkennung und Beseitigung komplexer Viren
- Während der Prüfung des Hauptspeichers werden aktive Viren gesperrt, bevor sie sich auf lokalen Datenträgern vervielfältigen. Böswillige Programme werden daran gehindert, Sicherheitslücken anderer Anwendungen bzw. des Betriebssystems auszunutzen.
- Erkennung und Beseitigung von Viren, die nur im Hauptspeicher existieren und nicht als Dateien vorkommen (Slammer und CodeRed)

Schutz vor unbekannten Bedrohungen

- **FLY-CODE** ist eine einzigartige Technologie für die Entpackung von Dateien, die auch unbekannte Packformate unterstützt
- Die Technologie der Nicht-Signatursuche **Origins Tracing™** sorgt dafür, dass die noch nicht eingetragenen Bedrohungen entdeckt werden können
- Durch Dr.Web Heuristik werden alle verbreiteten Virenbedrohungen entdeckt und nach ihren jeweiligen Kennungen klassifiziert

© Doctor Web, 2016

Technologien der Spam-Filterung

Dr.Web Antispam analysiert E-Mails anhand mehrerer tausend Regeln, die in verschiedene Gruppen aufgeteilt werden können.

Heuristische Analyse

Eine außerordentlich komplizierte und hochintelligente Technologie der empirischen Analyse aller E-Mail-Teile: E-Mail-Kopf, E-Mail-Körper usw. Dabei wird nicht nur die E-Mail, sondern auch der Inhalt angehängter Dateien analysiert. Die Heuristik erkennt sogar unbekannte Spam-Arten, wird permanent verbessert und um neue Regeln erweitert.

Filterung von Evasions-Techniken

Filterung von Evasions-Techniken ist eine der fortschrittlichsten und effizientesten Dr.Web Antispam-Technologien. Sie erkennt verschiedene Evasions-Techniken, die Spammer beim Umgehen der Antispam-Filter verwenden.

Analyse anhand HTML-Signaturen

E-Mails mit HTML-Code werden mit Mustern der HTML-Signaturen in der Spam-Datenbank verglichen. Ein solcher Vergleich in Kombination mit vorhandenen Daten über Bildgrößen, die Spammer oft verwenden, schützt Anwender vor Spam-Mails mit HTML-Code, in die häufig Online-Bilder eingebettet werden.

Erkennung von Spam anhand von E-Mail-Adressen

Die Erkennung von gefälschten E-Mails anhand von Signaturen auf SMTP-Servern und anderen Kennungen in E-Mail-Köpfen ist die neueste Methode im Kampf gegen Spam. Die Übeltäter können die E-Mail-Adresse des Absenders leicht verfälschen. Gefälschte E-Mails enthalten nicht nur Spam. Es können anonyme E-Mails und E-Mails sein, die Bedrohungen enthalten. Die Spezialtechnologien von Dr.Web Antispam ermöglichen es, dass gefälschte E-Mail-Adressen entdeckt und nicht durchgelassen werden. So ist Ihr Personal gegen E-Mails geschützt, die Ihre Mitarbeiter zu unberechenbaren Folgen bewegen können.

Semantische Analyse

Bei dieser Analyse werden Wörter und Redewendungen einer E-Mail mit den für die Spam-Mail spezifischen Kennungen verglichen. Der Vergleich erfolgt anhand eines Wörterbuches. Der Analyse werden sowohl sichtbare als auch unsichtbare Ausdrücke und Symbole unterzogen.

Anti-Betrug-Technologie

Betrugs-Mails (u.a. Farming-Mails) sind die gefährlichsten Spam-Mails. Dazu gehören auch der Nigeria-Scam, unverhoffte Lotterie- und Casinogewinne, gefälschte Bankbriefe. Für die Filterung von Scam-Mails ist in Dr.Web Antispam ein Spezialmodul verantwortlich.

Filterung des technischen Spams

Die sogenannten Bouncemeldungen entstehen als Reaktion auf Viren oder kommen in Form der Virenaktivität zutage: Selbstversender der E-Mail-Würmer bzw. E-Mails über eine fehlgeschlagene Zustellung. Ein Antispam-Modul stuft solche E-Mails als unerwünschte Korrespondenz ein.

Vorteile von Dr.Web Antispam

- Das Antispam-Modul braucht nicht erprobt und konfiguriert zu werden. Im Vergleich zu Antispam-Programmen, die die Bayes-Analyse verwenden, ist Dr.Web Antispam nicht lernbedürftig und startet die Bearbeitung mit dem Eingang der ersten E-Mail. Eine tägliche Administration ist daher nicht erforderlich.
- Keine Verlangsamung der E-Mail-Zustellung
- Filterung von E-Mails in Echtzeit
- Hohe Filterungsgeschwindigkeit bei geringen Systemanforderungen
- Bearbeitung von Objekten beliebiger Rekursionstiefe

© Doctor Web, 2016

- Auswahl einer passenden Technologie zur Bearbeitung eines bestimmten Objektes je nach E-Mail und blockierendem Objekt „on the fly“
- Vorsortierte E-Mails werden nicht gelöscht, sondern in ein Spezialverzeichnis verschoben, wo sie auf eventuelle Fehler überprüft werden können
- Auf Blacklists kann man verzichten: Die Schädigung des Unternehmensrufes ist dadurch nicht möglich
- Absolut autonom: Eine permanente Verbindung mit dem Server oder der Zugriff auf die Datenbank ist nicht erforderlich
- Update nicht häufiger als einmal pro Tag (große und häufige Updates sind ausgeschlossen)

Aufbau der Dr.Web Virendatenbank

Dr.Web verfügt im Vergleich zu anderen Antivirenprogrammen über die kleinste Größe der Virendatenbank. Dies ist der auf einer flexiblen Sprache basierenden hauseigenen Technologie zu verdanken, die für die Dr.Web Virendatenbank gedacht ist. Eine kleine Größe der Virendatenbank sorgt für einen geringen Internet-Verkehr und beansprucht weniger Platz auf der Festplatte und im Hauptspeicher. Dadurch können auch Komponenten des Dr.Web Antivirenprogramms schneller interagieren und keine überhöhte Serverauslastung hervorrufen.

Was ist die Hauptaufgabe eines Antivirenprogramms? Der Virenschutz!

Der Virenschutz wird durch die Eintragung von Signaturen in die Virendatenbank gewährleistet.

Die Zahl an Virensignaturen vermittelt uns keine Vorstellung davon, wie viele Viren von einem Antivirenprogramm erkannt und beseitigt werden können. Um zu begreifen, warum die Anzahl von Signaturen in der Dr.Web Virendatenbank weniger ist, als in den Virendefinitionsdateien anderer Hersteller, muss man wissen, dass nicht alle Viren einzigartig sind. Es gibt ganze Familien von gleichen Viren und Viren, die von Konstruktoren erstellt wurden. Andere Hersteller tragen für jeden Zwilling eine Signatur ein und machen ihre Virendatenbanken größer. Ein anderes Prinzip gilt für die Dr.Web Virendatenbank, in der sich mit einer Signatur dutzende, hunderte und manchmal auch tausende gleiche Viren entdecken lassen.

Vorteile der Dr.Web Virendatenbank

- Minimale Anzahl an Signaturen
- Kleine Größe von Updates
- Mit einer Signatur können hunderte und sogar tausende gleiche Viren entdeckt werden

Im Unterschied zu Konkurrenzprogrammen kann bei einer geringeren Anzahl an Signaturen die gleiche und sogar größere Zahl an Viren und Malware entdeckt werden.

Welchen Vorteil hat die geringe Größe der Dr.Web Virendatenbank und eine geringere Anzahl an Virensignaturen für den Anwender?

- Es wird ein geringer Speicherplatz auf der Festplatte benötigt
- Geringere Auslastung des Arbeitsspeichers
- Geringer Verkehr beim Herunterladen der Virendatenbank
- Schnelle Installation der Datenbank und promptes Abrufen von Daten bei der Virenanalyse
- Möglichkeit der Erkennung und Beseitigung unbekannter Viren, die durch die Modifikation bekannter Viren erstellt werden

Globales Dr.Web Update-System (Dr.Web GUS)

- Der Virenüberwachungsdienst von Doctor Web sammelt weltweit Virenkennungen, sucht Virensignaturen und veröffentlicht Updates nach der Analyse jeder neuen Bedrohung (in der Regel mehrmals pro Stunde)

© Doctor Web, 2016

- Nach der Veröffentlichung sind alle Updates auf mehreren Servern in verschiedenen Regionen der Welt verfügbar
- Um Fehler bei der Erkennung und Beseitigung von Malware zu vermeiden, werden sämtliche Updates an einer Vielzahl von sauberen Dateien getestet
- Das Update der Virendatenbanken und Programm-Module läuft automatisch
- Updates können als archivierte Dateien heruntergeladen werden

Lizenzen & Zertifikate

Im Unterschied zu den meisten Konkurrenzprogrammen verfügt Dr.Web Antivirensoftware über Konformitätszertifikate des Föderalen Dienstes für technische Überwachung und Exportkontrolle und des Föderalen Sicherheitsdienstes. So kann die Antivirensoftware in Unternehmen mit höheren Sicherheitsanforderungen verwendet werden.

Dr.Web ist das einzige vom Verteidigungsministerium der Russischen Föderation zertifizierte Antivirenprogramm.

Dr.Web entspricht dem Datenschutzgesetz und kann in Netzwerken verwendet werden, die das höchste Sicherheitsniveau voraussetzen.

Doctor Web verfügt zur Zeit über folgende Lizenzen und Zertifikate:

- Lizenzen des Föderalen Dienstes für technische Überwachung und Exportkontrolle der Russischen Föderation für die Entwicklung von IT-Sicherheitsprodukten
- Lizenz des Verteidigungsministeriums der Russischen Föderation für die Entwicklung von IT-Sicherheitsprodukten
- Lizenzen des Föderalen Sicherheitsdienstes der Russischen Föderation für Arbeiten, die mit dem Staatsgeheimnis verbunden sind
- Lizenz des Lizenzierungszentrums des Föderalen Sicherheitsdienstes für die Entwicklung von IT-Sicherheitsprodukten
- Konformitätszertifikat des Föderalen Sicherheitsdienstes der Russischen Föderation
- Konformitätszertifikat des Föderalen Dienstes für technische Überwachung und Exportkontrolle der Russischen Föderation

Alle Lizenzen und Zertifikate von Doctor Web

http://company.drweb-av.de/licenses_and_certificates/

© Doctor Web, 2016

Dr.Web Lizenzzertifikat

LIZENZZERTIFIKAT

Dr.WEB®

Das vorliegende Lizenzzertifikat bestätigt, dass diese Software von **Doctor Web**, dem Hersteller und Inhaber von Urheberrechten für **Dr.WEB** Sicherheitsprodukte, lizenziert wurde.

Lizenzinhaber
Lizenziertes Produkt
Seriennummer
Seriennummer
Seriennummer
Geschützte Objekte

Workstations	Server
E-Mail-Anwender	Gateway-Anwendera
Mobile Endgeräte	Verwaltungscenter

Laufzeit	Lieferant

Boris Scharov
Generaldirektor
der Doctor Web Ltd.

«Доктор Веб»
«Doctor Web» Ltd.

Das Dr.Web Lizenzzertifikat ist ein Beleg für die gesetzmäßige Nutzung der Dr.Web Software und ist entsprechenden Aufsichtsbehörden vorzuweisen.

WICHTIG! Das Dr.Web Lizenzzertifikat gewährt keine Berechtigung für die Lizenzverlängerung und Verlängerungsrabatte.

Das Lizenzzertifikat ist sicher geschützt und kann nicht verfälscht werden.

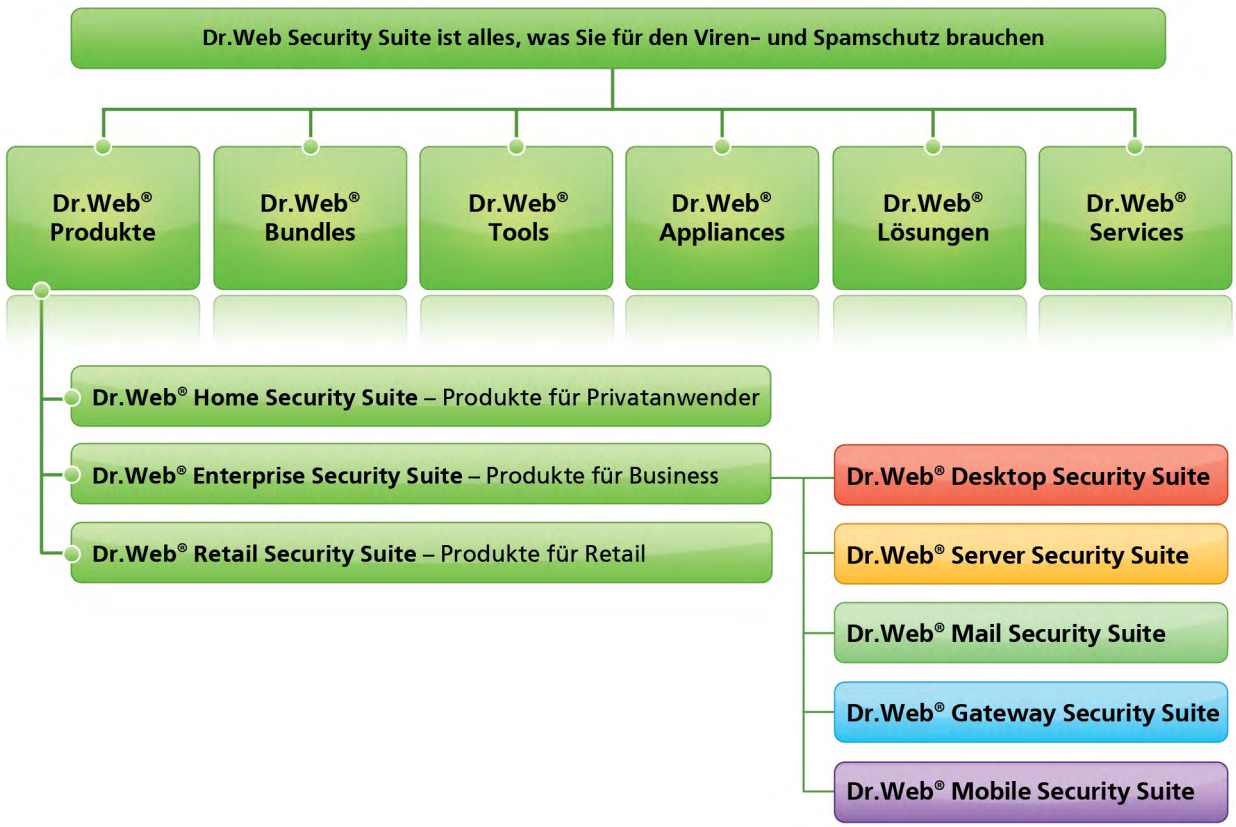
Die Vorlage eines Lizenzzertifikats wird mit Dr.Web Produkten geliefert und ist obligatorisch für Unternehmen!

Die elektronische Kopie des Dr.Web Lizenzzertifikats kann auf der folgenden Webseite https://products.drweb-av.de/register/certificate/?lng=de generiert werden.

© Doctor Web, 2016

Produktpalette Dr.Web Security Suite

Die Produktpalette Dr.Web Security Suite besteht aus kommerziellen Produkten für Privat, Business und Retail, Tools, Appliances, Lösungen und Services.



Lizenzierung

1. Dr.Web Produkte werden für 12, 24 und 36 Monate lizenziert. Dr.Web Security Space und Dr.Web Antivirus für Windows werden auch für 3 und 6 Monate lizenziert.
2. Die Lizenzierung von Dr.Web Produkten richtet sich je nach Typ des zu schützenden Objektes.
3. Die zu schützenden Objekte umfassen:
   - Workstations, Clients der Terminalserver und integrierte Systeme
   - Datei- und Anwendungsserver (einschließlich der Terminalserver)
   - E-Mail-Anwender
   - Anwender von E-Mail- und Internet-Gateways
   - Mobile Endgeräte

© Doctor Web, 2016

4. Es sind 2 **Basislizenzen** vorgesehen:
   1) Antivirus (mit einer Firewall)
   2) Rundumschutz
5. Die Basislizenz **Rundumschutz** ist nur für Produkte für Workstations vorgesehen.
6. Die Lizenz **Rundumschutz** enthält folgende Komponenten: Antivirus, Antispam, Web-Antivirus, Elterliche Kontrolle (Office Control), Firewall.
7. Die nötigen Schutzkomponenten werden in die Basislizenz mit aufgenommen. Der Verkauf der separaten Lizenz für eine oder mehrere Schutzkomponenten ist nicht möglich.
8. Für jede Art des zu schützenden Objektes sind Basislizenzen und entsprechende Schutzkomponenten vorgesehen.

Zu schützende Objekte	Unterstützte Systeme und Plattformen	Basislizenz	Zusätzliche Schutzkomponenten
Dr.Web Desktop Security Suite Workstations Clients der Terminalserver Clients virtueller Server Clients integrierter Systeme	Windows XP/2003/Vista/2008/7/8/2012/10 (32 und 64 Bit)	Rundumschutz	■ Verwaltungscenter
		Antivirus	
	OS X 10.7 und höher Linux glibc 2.13 und höher	Antivirus	■ Verwaltungscenter
	Konsolen-Scanner		
Dr.Web Server Security Suite Dateiserver Anwendungsserver Terminalserver Virtuelle Server	Windows OS X Server Novell NetWare UNIX (Samba)	Antivirus	■ Verwaltungscenter
Dr.Web Mail Security Suite E-Mail-Anwender	UNIX MS Exchange	Antivirus	■ Verwaltungscenter ■ Antispam ■ SMTP-Proxy
	Lotus (Windows/Linux)		■ Antispam ■ SMTP-Proxy
	Kerio (Windows/Linux)		■ SMTP-Proxy
Dr.Web Gateway Security Suite Anwender von Internet-Gateways	Internet-Gateways Kerio Internet-Gateways UNIX	Antivirus	■ Verwaltungscenter
	Dr.Web für Microsoft ISA Server und Forefront TMG Qbik WinGate MIMEsweeper		■ Antispam
Dr.Web Mobile Security Suite Mobile Endgeräte	Android	Rundumschutz	■ Verwaltungscenter ■ Antispam
	Symbian OS	Antivirus	■ Antispam
	Windows Mobile		

© Doctor Web, 2016

Lieferarten für Dr.Web Produkte

1. Dr.Web E-Lizenz

Wird als Dr.Web Seriennummer geliefert:

- per E-Mail
- mit dem Lizenzzertifikat

2. Dr.Web Mediapaket in der Kartonpackung

Lieferumfang:

- Firmenpackung
- Lizenzzertifikat
- Kurzanleitung für die Registrierung und Installation
- DVD
- Briefumschlag für CD
- Aufkleber
- Aufkleber „Geschützt mit Dr.Web“
- USB-Speicher (nur für Dr.Web für OS X + Dr.Web Security Space)

3. Lösung in der Kartonpackung

Individuell konfigurierbare Lösung für eines oder mehrere Produkte von Dr.Web Enterprise Security Suite.

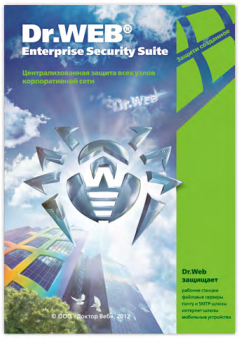
Lieferumfang:

- Dr.Web Firmenpackung
- Vorlage des Lizenzvertrags
- DVD mit Dr.Web Distributionsdateien in einem Umschlag

© Doctor Web, 2016

4. Dr.Web Lizenzpaket

Individuell konfigurierbare Lösung für eines oder mehrere Produkte von Dr.Web Enterprise Security Suite.



Lieferumfang:

- Dr.Web Firmenpaket
- Vorlage des Lizenzvertrags

5. Scratch-Karte

Karte mit der Dr.Web Seriennummer unter einem Rubbel-Streifen.

6. Dr.Web OEM-Karten

Dr.Web Security Space

1 PC / 3 Monate

- OEM-Karte mit einem Rubbel-Streifen in der OEM-Broschüre

Nach Vereinbarung können OEM-Karten mit einem Partnerlogo hergestellt werden.

Minimale Anzahl: 5 000 Stück.

© Doctor Web, 2016

Dr.Web Home Security Suite: Produkte für Privatanwender

Produktumfang

Dr.Web Security Space	Dr.Web Mobile Security
Schutz für beliebige Endgeräte	Schutz für mobile Endgeräte
Dr.Web Produkte	
■ Dr.Web Security Space ■ Dr.Web Antivirus für Windows ■ Dr.Web Antivirus für OS X ■ Dr.Web Antivirus für Linux	–
■ Dr.Web für Android ■ Dr.Web für Symbian ■ Dr.Web für Windows Mobile	■ Dr.Web für Android ■ Dr.Web für Symbian ■ Dr.Web für Windows Mobile

Schutzkomponenten von Dr.Web Security Space

Schutzkomponenten	Windows	OS X	Linux
Antivirus	+	+	+
Antispam	+		
Web-Antivirus	+	+	
Kinderschutz	+		
Firewall	+		
Antivirus-Netzwerk	+		

Lizenzierung von Dr.Web Security Space

1. Das Produkt wird nach der Anzahl der zu schützenden Rechner (1-5) lizenziert
2. Lizenzierungsvarianten: Rundumschutz
3. Laufzeit: 3, 6, 12, 24 oder 36 Monate / Laufzeit von OEM-Lizenzen: 3 oder 6 Monate
4. Es gelten die üblichen Rabatte für die Lizenzverlängerung
5. Es sind keine weiteren Rabatte vorgesehen
6. Die Käufer von Dr.Web Security Space können Dr.Web Mobile Security Suite kostenlos nutzen. Die Anzahl der zu schützenden mobilen Endgeräte entspricht der Anzahl der zu schützenden PCs.

Lizenzerweiterung

1. Die Lizenzerweiterung für Dr.Web Security Space besteht entweder im Umstieg von Dr.Web Antivirus auf Dr.Web Security Space oder in der Erhöhung der Anzahl zu schützender Objekte.
2. Die erweiterte Lizenz wird bei der Generierung automatisch aktiviert.
3. Wenn die zu erweiternde Lizenz eine Restlaufzeit von **mehr als 3 Monaten** hat, erfolgt die Lizenzerweiterung zum Preis einer Lizenzverlängerung (Lizenztyp-Code: D). Die Lizenz wird automatisch verlängert.
4. Wenn die zu erweiternde Lizenz eine Restlaufzeit von **weniger als 3 Monaten** hat:
   - Die Lizenzerweiterung erfolgt über den kostenfreien Lizenzverlängerungsservice
   - Die vorherige Lizenz wird in 24 Stunden nach der Generierung der neuen Lizenz blockiert
   - Typ der neuen Lizenz: C. Diese Lizenz ist kostenlos. Sie kann später mit einem Preisvorteil verlängert werden.

© Doctor Web, 2016

Dr.Web Security Space

Rundumschutz für Windows, Antivirus für OS X und Linux

- Rundumschutzlösung für Ihren Computer
- Rundumschutzlösung für Ihren PC unter Windows
- Schutz vor Viren & Co. in Echtzeit
- Installation auf einem bereits infizierten PC möglich
- Hohe Resistenz gegenüber Viren
- Effiziente Erkennung von Malware und Systemreinigung
- Hoher Durchsatz durch Multithreading
- Schutz vor neuen Schädlingen, welche Signatursuche und Heuristik umgehen können
- Schutz vor Datenbeschädigung
- Rundumanalyse gepackter Bedrohungen
- Rekursive Prüfung von Archiven
- Hervorragende Erkennung und Neutralisierung komplexer Viren & Co.
- Filterung von Spam-Mails und unerwünschter Nachrichten ohne Training des Antispam-Moduls
- Vollständige Prüfung von aus dem Internet heruntergeladener Daten in Echtzeit
- Sicheres Surfen auf Suchmaschinen wie Google, Yandex, Yahoo!, Bing, Rambler, etc. durch die Funktion „Sicheres Suchen“
- Sicheres Chatten durch Filterung von Instant Messaging-Nachrichten
- Schutz vor jugendgefährdenden Web-Inhalten
- Sperrung unerlaubter Zugriffe auf Wechseldatenträger und ausgewählte Bereiche der Festplatte
- Dr.Web Cloud zur Prüfung von URLs durch Server von Doctor Web
- Schutz vor Remote-Zugriffen und Datendiebstahl durch Sperrung verdächtiger Netzwerkverbindungen auf Paket- und Anwendungsebene
- Fernsteuerung von Dr.Web auf anderen PCs im lokalen Netzwerk ohne Dr.Web Verwaltungscenter

Schutzkomponenten

Effiziente Erkennung von Bedrohungen aller Art (Dr.Web Virenscanner)

- Höherer Scan-Durchsatz durch eine mehrströmige Daten-Bearbeitung und einen vollen Einsatz von Multiprozessorsystemen
- Bequeme und intuitiv verständliche Benutzeroberfläche
- Schnelle und sorgfältige Prüfung des Hauptspeichers, der Boot-Sektoren, Festplatten und Wechseldatenträger
- Neutralisierung von Viren, Trojanern und sonstiger Malware
- Umfangreiche Virendatenbanken zur Erkennung und Beseitigung von Spyware, Riskware, Adware, Hackertools und Scherzprogrammen
- Der Konsolenscanner ist für fortgeschrittene Anwender gedacht und ermöglicht eine Prüfung im Kommandozeilen-Modus. Er bietet vielfältige Konfigurationsmöglichkeiten und kann auch in Multiprozessorsystemen eingesetzt werden.

Echtzeitschutz (Datei-Wächter SpIDer Guard®)

- Die Leistung auf Rechnern mit hohem Datendurchsatz (beim Herunterladen von Torrent- und Sharing-Trackern sowie beim Kompilieren und Rendering) durch die Überholung von Dr.Web SpIDer Guard
- Ständige Überwachung der Sicherheitslage des PCs: Kontrolle der Dateizugriffe auf lokalen Datenträgern, Floppys, CD-/DVD-/ und Blue-Ray-Laufwerken, Flash-Speichern und Smartcards
- Hohe Resistenz gegenüber Evasions-Techniken

© Doctor Web, 2016

Schutz vor Rootkits (Antirootkit-Modul Dr.Web Shield™)

- Sicherer Schutz vor Viren, die Rootkit-Techniken verwenden
- Neutralisierung komplexer Viren (Shadow.based (Conficker), MaosBoot, Rustock.C, Sector)

E-Mails ohne Viren & Co. (E-Mail-Wächter SpIDer Mail®)

- Sicherer E-Mail-Traffic: Die über vorhandene Ports und unterstützte Protokolle (u.a. geschützte Protokolle, wenn der Benutzer SSL aktiviert) übertragenen Daten werden geschützt
- Prüfung von E-Mails, die via SMTP/POP3/NNTP/IMAP4 abgerufen werden. Der E-Mail-Wächter schont Systemressourcen. Der Eingang von E-Mails wird nicht verlangsamt.
- Prüfung von verschlüsselten SSL-Verbindungen, die via SMTPS/POP3S/IMAP4S hergestellt werden
- Der E-Mail-Client kann einwandfrei funktionieren und E-Mails ohne Verlangsamung empfangen
- Individuelle Behandlungsregeln für jede einzelne Spielart von Malware: Viren, Riskware, Hackertools, Dialer und Scherzprogramme
- Schutz vor Viren-Mails, die durch E-Mail-Würmer massenhaft versendet werden. Durch die Analyse des E-Mail-Körpers und der Absendezeit ausgehender E-Mails werden böswillige E-Mails aussortiert.

E-Mails ohne Spam und unerwünschte E-Mails (Dr.Web Antispam)

- Prüfung ein- und ausgehender E-Mails erfolgt in Echtzeit
- Das Antispam-Modul ist mit allen vorhandenen E-Mail-Programmen kompatibel. Der Eingang von E-Mails wird nicht verlangsamt.
- Das Antispam-Modul erfordert keine Konfiguration durch den Benutzer und ist mit dem Eingang der ersten E-Mail einsatzbereit
- Verschiedene Filterungstechnologien sorgen für hohe Erkennungsrate bei Spam-, Phishing-, Scam- und Bounce-Mails
- Schutz vor Botnets: Die Internetabschaltung durch Ihren Internetanbieter wegen Spam-Versands ist ausgeschlossen
- Abgefilterte E-Mails werden nicht gelöscht, sondern in Quarantäne verschoben, wo sie jederzeit auf eventuelle Fehler geprüft werden können
- Dr.Web Antispam läuft autonom. Für das Antispam-Modul ist die Verbindung zu einem externen Server sowie einer Datenbank nicht erforderlich. Der Internet-Traffic wird verringert.

Schutz von E-Mails, die durch Microsoft® Outlook übertragen werden

- Das Modul Dr.Web für Outlook überprüft angehängte Dateien sowie E-Mails, die per SSL übertragen werden auf Viren, filtert Spam-Mails aus und entdeckt und neutralisiert böswillige Software. Darüber hinaus wird die Dr.Web Heuristik als zusätzliche Schutzkomponente gegen unbekannte Viren eingesetzt.

Dr.Web LinkChecker: Virenprüfung und Suche in der Datenbank für unerwünschte Websites ohne Installation von Dr.Web Security Space

- Antivirus-Plug-ins zur Prüfung von Webseiten und Dateien aus dem Internet sowie Links in E-Mails, die durch Mozilla Thunderbird bearbeitet werden. All diese Optionen sind ohne Installation von Dr.Web Antivirus verfügbar.
- Die Plug-ins ermöglichen das Abrufen von Webseiten und benachrichtigen Sie, wenn Sie auf externe Links in sozialen Netzwerken wie Facebook, Google+ usw. klicken. Die Plug-ins scannen diese Links und Dateien aus dem Internet, entdecken und überprüfen modifizierte Links und kontrollieren diese auf Skripts und Frames.

Schutz gegen Internetbedrohungen (Web-Antivirus SpIDer Gate™)

- SpIDer Gate™ scannt in Echtzeit den eingehenden HTTP-Verkehr, fängt alle HTTP-Verbindungen ab, filtert Daten, sperrt automatisch infizierte Websites in jedem Webbrowser, überprüft Dateien in

© Doctor Web, 2016

Archiven (die z.B. über den Upload-Manager heruntergeladen werden) und schützt vor Phishing-Websites sowie anderen gefährlichen Web-Inhalten

- Sicherer Internet-Traffic: Die über vorhandene Ports und unterstützte Protokolle (u.a. geschützte Protokolle, wenn der Benutzer SSL aktiviert) übertragenen Daten werden geschützt
- **Sicheres Surfen im Internet.** Unter den Treffern der Suchmaschinen wie Google, Yandex, Yahoo!, Bing und Rambler werden dank der Funktion „Sicheres Suchen" nur sichere Websites angezeigt. Unsichere Inhalte werden von Suchmaschinen ausgenommen.
- **Sichere Kommunikation.** Die über Instant-Messaging-Systeme wie Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin usw. übertragenen Daten werden auf Malware gefiltert. Links, die auf Malware- oder Piraten-Websites weiterleiten, werden ausgeschnitten. Dateianhänge werden geprüft und bei Virenfund blockiert.
- Prüfung von verschlüsselten SSL-Verbindungen (HTTPS)
- Datenbank von Websites, die nicht lizenzierte Inhalte verbreiten (Schutz für Urheber)
- Der ein- und ausgehende Verkehr kann deaktiviert werden. Außerdem können Sie eine Liste von Anwendungen erstellen, deren HTTP-Verkehr in jedem Fall und vollständig geprüft werden soll (Blacklist). Sie können auch den Verkehr von der Prüfung ausnehmen (Whitelist).
- Einstellung der Scan-Priorität: Die Balancierung beeinflusst die Verteilung der CPU-Auslastung und die Internetgeschwindigkeit
- SpIDer Gate™ ist mit jedem Webbrowser kompatibel
- Die Datenfilterung erfolgt ressourcenschonend und verlangsamt die Internetgeschwindigkeit sowie den Umfang übertragener Daten nicht
- Im Default-Modus ist keine weitere Konfiguration des Moduls erforderlich: Dr.Web SpIDer Gate™ ist sofort nach der Installation einsatzbereit
- URL-Prüfung auf Servern von Doctor Web durch Dr.Web Cloud. Beim Aufrufen von Websites werden URLs auf Servern von Doctor Web geprüft. Die Virenprüfung erfolgt in Echtzeit und unabhängig vom Stand der Dr.Web Virendatenbank auf dem PC des Benutzers und den Update-Einstellungen.

Überwachung von Web-Inhalten (Dr.Web Elterliche Kontrolle)

- Sicherer Internet-Traffic: Es werden Daten, die über alle vorhandenen Ports übertragen werden, geprüft
- Kinderschutz vor unerwünschten Web-Inhalten
- Sperrung der Modifikation der Systemzeit und Zeitzone. Der Nachwuchs kann den Zugang zum PC nur während der erlaubten Zeitperiode haben.
- Blockierung von gefährlichen Websites, die in 10 thematische Gruppen aufgeteilt sind (Waffen, Drogen, Glücksspiele, Pornografie usw.)
- Sperren von Wechseldatenträgern (Flash-Speicher, USB-Geräte), Netzwerk-Geräten sowie einzelnen Dateien und Verzeichnissen. Dies ist eine weitere Möglichkeit, sensible Daten vor dem Entfernen bzw. Diebstahl durch Kriminelle zu schützen.
- Die Whitelist schützt Ihren Rechner vor unerlaubtem Verwenden von Wechseldatenträgern sowie Ihre Daten vor Diebstahl und schiebt Viren & Co. einen Riegel vor. Neu! Export/Import von Whitelists.
- URL-Prüfung auf Servern von Doctor Web durch Dr.Web Cloud in Echtzeit, unabhängig vom Stand der Dr.Web Virendatenbank auf dem PC des Benutzers und den Update-Einstellungen
- Sperrung von Druckaufgaben: Das unerlaubte Ausdrucken von sensiblen Daten wird gesperrt

Schutz vor Internetangriffen (Dr.Web Firewall)

- Schutz vor unerlaubtem Zugriff von außen und Datendiebstahl. Blockierung verdächtiger Verbindungen auf Paket- und Applikationsebene.
- Die neue Regeldatenbank der Dr.Web Firewall bietet noch mehr Komfort für Benutzer bei der Erstellung von Regeln. Zur Zeit verwendet die Dr.Web Firewall die eigene Regeldatenbank für vertrauenswürdige Anwendungen. Die Vertrauenswürdigkeit einer Anwendung basiert auf einem gültigen

© Doctor Web, 2016

Zertifikat. Alle Programme, die von Dr.Web akzeptiert werden, können eine Verbindung mit beliebigen Adressen über beliebige Ports aufbauen. Ausnahme: Wenn die Anwendung keine gültige oder überhaupt keine Signatur hat, wird nach der Erstellung einer Regel für diese Anwendung gefragt.

- Die Kontrolle von Verbindungen auf Applikationsebene ermöglicht die Überwachung des Zugriffs jeweiliger Programme und Prozesse auf Netz-Inhalte. Sämtliche Zugriffe werden protokolliert.
- Die Filterung auf Paketebene ermöglicht die Kontrolle des Internetzugriffs unabhängig von Programmen, die die Verbindung initiieren. Im Protokoll des Paketfilters werden Paketdaten gespeichert, die über Netzoberflächen übertragen werden.
- Sie können einen Spielmodus aktivieren, bei dem ein Fenster zur Erstellung von Regeln oberhalb einer beliebigen Anwendung erscheint
- Überwachung von Anwendungen, die das Netzwerk in Echtzeit verwenden, mit der Möglichkeit, eine Verbindung abzubrechen

Remote-Verwaltung

- Durch die Komponente Antivirus-Netzwerk können Dr.Web Antivirenprogramme auf PCs in einem lokalen Netzwerk verwaltet werden
- Zur Remote-Verwaltung ist die Installation des Dr.Web Verwaltungscenters nicht erforderlich
- Sie können eine Verbindung zu einem beliebigen PC im lokalen Netzwerk herstellen
- Die Verwaltungsmöglichkeiten umfassen: Erstellung von Statistiken und Protokollen, Einsehen und Konfiguration von Einstellungen der Module sowie Start und Abbrechen der Module. Für den Remote-Computer sind auch die Registrierung einer Seriennummer und das Auswechseln einer Schlüsseldatei möglich.
- Für einen Remote-Zugang ist dessen Freigabe auf dem Zielcomputer erforderlich

Unterstützte Betriebssysteme

- Windows XP/2003/Vista/2008/7/8/2012/10 (32 und 64 Bit)
- HDD: ~450 MB. Für temporäte Dateien, die während der Installation erstellt werden, ist ein Freiplatz erforderlich

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/win/security_space/

Dr.Web Antivirus für Windows

Minimal erforderlicher Schutz vor Viren & Co. für Windows, OS X, Linux

- Rundumschutzlösung für Ihren PC unter Windows
- Schutz vor Viren & Co. in Echtzeit
- Installation auf einem bereits infizierten PC möglich
- Hohe Resistenz gegenüber Viren
- Effiziente Erkennung von Malware und Systemreinigung
- Hoher Durchsatz durch Multithreading
- Schutz vor neuen Schädlingen, welche Signatursuche und Heuristik umgehen können
- Schutz vor Datenbeschädigung
- Rundumanalyse gepackter Bedrohungen
- Rekursive Prüfung von Archiven
- Hervorragende Erkennung und Neutralisierung komplexer Viren & Co.
- Filterung von Spam-Mails und unerwünschter Nachrichten ohne Training des Antispam-Moduls
- Vollständige Prüfung von aus dem Internet heruntergeladener Daten in Echtzeit
- Sperrung unerlaubter Zugriffe auf Wechseldatenträger und ausgewählte Bereiche der Festplatte

© Doctor Web, 2016

Schutzkomponenten

Effiziente Erkennung von Bedrohungen aller Art (Dr.Web Virenscanner)

- Der Dr.Web Scanner ermöglicht einen höheren Scan-Durchsatz durch eine mehrströmige Prüfung und einen vollen Einsatz von Multiprozessorsystemen. Die Leistung des Scanners ist im Vergleich zur Vorgängerversion wesentlich gestiegen.
- Neue Benutzeroberfläche des Dr.Web Scanners
- Schnelle und sorgfältige Prüfung des Hauptspeichers, der Boot-Sektoren, Festplatten und Wechseldatenträger
- Neutralisierung von Viren, Trojanern und sonstiger Malware
- Umfangreiche Virendatenbanken zur Erkennung und Beseitigung von Spyware, Riskware, Adware, Hackertools und Scherzprogrammen
- Der Konsolenscanner ist für fortgeschrittene Anwender gedacht und ermöglicht eine Prüfung im Kommandozeilen-Modus. Er bietet vielfältige Konfigurationsmöglichkeiten und kann auch in Multiprozessorsystemen eingesetzt werden.

Echtzeitschutz (Datei-Wächter SpIDer Guard®)

- Ständige Überwachung der Sicherheitslage des PCs: Kontrolle der Dateizugriffe auf lokalen Datenträgern, Floppys, CD-/DVD-/ und Blue-Ray-Laufwerken, Flash-Speichern und Smartcards
- Hohe Resistenz gegenüber Evasions-Techniken
- Die Leistung auf Rechnern mit hohem Datendurchsatz (beim Herunterladen von Torrent- und Sharing-Trackern sowie beim Kompilieren und Rendering) durch die Überholung von Dr.Web SpIDer Guard

Schutz vor Rootkits (Antirootkit-Modul Dr.Web Shield™)

- Sicherer Schutz vor Viren, die Rootkit-Techniken verwenden
- Neutralisierung komplexer Viren (Shadow.based (Conficker), MaosBoot, Rustock.C, Sector)

E-Mails ohne Viren & Co. (E-Mail-Wächter SpIDer Mail®)

- Sicherer E-Mail-Traffic: Die über vorhandene Ports und unterstützte Protokolle (u.a. geschützte Protokolle, wenn der Benutzer SSL aktiviert) übertragenen Daten werden geschützt
- Virenprüfung von E-Mails, die per SMTP/POP3/NNTP/IMAP4 übertragen werden
- Prüfung von verschlüsselten SSL-Verbindungen (SMTPS/POP3S/IMAP4S)
- Der E-Mail-Client kann einwandfrei funktionieren und E-Mails ohne Verlangsamung empfangen
- Besondere Behandlungsregeln für jede einzelne Spielart von Malware: Viren, Riskware, Hackertools, Dialer und Scherzprogramme
- Schutz vor Viren-Mails, die durch E-Mail-Würmer massenhaft versendet werden. Durch die Analyse des E-Mail-Körpers und der Absendezeit ausgehender E-Mails werden böswillige E-Mails aussortiert.

Schutz von E-Mails, die durch Microsoft® Outlook übertragen werden

- Das Modul Dr.Web für Outlook überprüft angehängte Dateien sowie E-Mails, die per SSL übertragen werden, auf Viren, filtert Spam-Mails aus und entdeckt und neutralisiert böswillige Software. Darüber hinaus wird die Dr.Web Heuristik als zusätzliche Schutzkomponente gegen unbekannte Viren eingesetzt.

Dr.Web LinkChecker: Virenprüfung und Suche in der Datenbank für unerwünschte Websites ohne Installation von Dr.Web Security Space

- Antivirus-Plug-ins zur Prüfung von Webseiten und Dateien aus dem Internet sowie Links in E-Mails, die durch Mozilla Thunderbird bearbeitet werden. All diese Optionen sind ohne Installation von Dr.Web Antivirus verfügbar.

© Doctor Web, 2016

- Die Plug-ins ermöglichen das Abrufen von Webseiten und benachrichtigen Sie, wenn Sie auf externe Links in sozialen Netzwerken wie Facebook, Google+ usw. klicken. Die Plug-ins scannen diese Links und Dateien aus dem Internet, entdecken und überprüfen modifizierte Links und kontrollieren diese auf Skripts und Frames.

Schutz vor Netzangriffen (Dr.Web Firewall)

- Schutz vor unerlaubtem Zugriff von außen und Datendiebstahl. Blockierung verdächtiger Verbindungen auf Paket- und Applikationsebene.
- Die neue Regeldatenbank der Dr.Web Firewall bietet noch mehr Komfort für Benutzer bei der Erstellung von Regeln. Zur Zeit verwendet die Dr.Web Firewall die eigene Regeldatenbank für vertrauenswürdige Anwendungen. Die Vertrauenswürdigkeit einer Anwendung basiert auf einem gültigen Zertifikat. Alle Programme, die von Dr.Web akzeptiert werden, können eine Verbindung mit beliebigen Adressen über beliebige Ports aufbauen. Ausnahme: Wenn die Anwendung keine gültige oder überhaupt keine Signatur hat, wird nach der Erstellung einer Regel für diese Anwendung gefragt.
- Die Kontrolle von Verbindungen auf Applikationsebene ermöglicht die Überwachung des Zugriffs jeweiliger Programme und Prozesse auf Netz-Inhalte. Sämtliche Zugriffe werden protokolliert.
- Die Filterung auf Paketebene ermöglicht die Kontrolle des Internetzugriffs, unabhängig von Programmen, die die Verbindung initiieren. Im Protokoll des Paketfilters werden Paketdaten gespeichert, die über Netzoberflächen übertragen werden.
- Sie können einen Spielmodus aktivieren, bei dem ein Fenster zur Erstellung von Regeln oberhalb einer beliebigen Anwendung erscheint
- Überwachung von Anwendungen, die das Netzwerk in Echtzeit verwenden, mit der Möglichkeit, eine Verbindung abzubrechen

Remote-Verwaltung

- Durch die Komponente Antivirus-Netzwerk können Dr.Web Antivirenprogramme auf PCs in einem lokalen Netzwerk verwaltet werden
- Zur Remote-Verwaltung ist die Installation des Dr.Web Verwaltungscenters nicht erforderlich
- Sie können eine Verbindung zu einem beliebigen PC im lokalen Netzwerk herstellen
- Die Verwaltungsmöglichkeiten umfassen: Erstellung von Statistiken und Protokollen, Einsehen und Konfiguration von Einstellungen der Module sowie Start und Abbrechen der Module. Für den Remote-Computer sind auch die Registrierung einer Seriennummer und das Auswechseln einer Schlüsseldatei möglich.
- Für einen Remote-Zugang ist dessen Freigabe auf dem Zielcomputer erforderlich

Unterstützte Betriebssysteme

- Intel® Pentium® IV mit 1,6 GHz
- Hauptspeicher: 512 MB. Für temporäre Dateien, die während der Installation erstellt werden, ist ein Zusatzplatz erforderlich.
- HDD: 330 MB
- Windows XP/2003/Vista/2008/7/8/2012/10 (32 und 64 Bit).
- OS X 10.7 oder höher (32 und 64 Bit)
- Linux 2.6.37 oder höher (32 und 64 Bit)
- Glibc 2.13 und höher (32 und 64 Bit)

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/win/

© Doctor Web, 2016

Dr.Web Antivirus für OS X

Schutz vor Viren & Co., die es nicht nur auf OS X, sondern auch auf andere Betriebssysteme abgesehen haben

Dieses Produkt ist in Lizenzen für Dr.Web Security Space und Dr.Web Antivirus enthalten

Vorteile

- Asynchrone Virenprüfung ermöglicht beliebige Aktionen mit Dateien. Durch geringe Systemauslastung läuft Dr.Web für OS X fast unsichtbar.
- Für Dr.Web für OS X ist das Aufhängen des Betriebssystems unmöglich, selbst wenn ein Fehler unterlaufen ist
- Die Voreinstellungen des Programms sorgen dafür, dass der Benutzer keine weiteren Schritte vornehmen muss und sich auf laufende Aufgaben konzentrieren kann
- Die stilvolle Benutzeroberfläche von Apple OS X Aqua macht die Arbeit mit Dr.Web leicht und intuitiv verständlich

Möglichkeiten

- Prüfung von Autostart-Dateien, Wechseldatenträgern, Netzwerk-Treibern und Logical Values, E-Mails sowie Dateien und Verzeichnissen (u.a. gepackt und archiviert)
- Auswahl eines Scanmodus: Schnell, vollständig und benutzerdefiniert
- Virenprüfung manuell, automatisch oder nach Zeitplan
- Passwortschutz des Wächters SpIDer Guard® vor unerlaubtem Zugriff
- Auswahl einer Aktion für infizierte, verdächtige und sonstige Objekte, einschließlich der Desinfektion, Verschiebung in die Quarantäne und der Entfernung (auch wenn die früher ausgewählte Aktion unmöglich war)
- Auslassen der Prüfung für Pfade und Dateien auf Anforderung
- Erkennung und Beseitigung von Viren, die durch unbekannte Packprogramme gepackt wurden
- Protokollierung des Zeitpunktes eines Ereignisses, des geprüften Objektes und einer Aktion
- Automatisches Update der Virendatenbanken und Programm-Module auf Anforderung oder nach Zeitplan
- Benachrichtigung (u.a. Ton-Benachrichtigung) über Virenereignisse
- Verschiebung infizierter Objekte in die Quarantäne mit der Option der Wiederherstellung und Einschränkung der Quarantäne-Größe
- Desinfektion, Wiederherstellung und Entfernung der in die Qurantäne verschobenen Objekte
- Detaillierte Protokollierung
- Verwendung von Modulen als Tools der Kommandozeile, Möglichkeit der Integration von Modulen in Apple Scripts-Systeme

Systemanforderungen

- OS X 10.7 und höher (32 und 64 Bit)
- Hauptspeicher gemäß Systemanforderungen
- Internetverbindung (für die Registrierung und das Herunterladen von Updates)

© Doctor Web, 2016

Dr.Web Antivirus für Linux

Minimal erforderlicher Virenschutz

Schlüsselfunktionen

- Erkennung und Beseitigung von Malware und böswilligen Objekten auf Festplatten und Wechseldatenträgern
- Erkennung und Beseitigung von Viren in Archiven beliebiger Rekursionstiefe und gepackten Objekten
- Prüfung von Dateien via FLY-CODE™, die durch bekannte sowie unbekannte Packprogramme komprimiert wurden
- Schutz vor unbekannten Viren durch die Nicht-Signatursuche Origins Tracing™ und Dr.Web Heuristik
- Verschiedene Prüfungsarten: Schnell, vollständig und benutzerdefiniert
- Permanente Kontrolle des Sicherheitsniveaus des PCs: Überwachung von Dateizugriffen auf Festplatten, Disketten, CD/DVD/Blu-ray-Laufwerken, Flash- und Smartcards
- Schutz vor Evasions-Techniken
- Verschiebung infizierter Objekte in die Quarantäne mit der Option der Wiederherstellung und Einschränkung der Quarantäne-Größe
- Sammlung von Statistiken
- Automatisches Update auf Anforderung oder nach Zeitplan

Vorteile

- Komfortables Verwaltungscenter
- Prüfung „on the fly“
- Benutzerdefinierte Prüfung
- Verwaltbare Quarantäne
- Automatisches Update
- Stilvolle Benutzeroberfläche

Systemanforderungen

- Betriebssystem: GNU/Linux-Installationsdateien unter Intel x86/amd64 auf Basis der Engine 2.6.37 (und höher) mit der glibc-Bibliothek 2.13 (und höher).
- HDD: mind. 512 MB
- Internetverbindung für Updates.

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/linux/

© Doctor Web, 2016

Dr.Web Konsolen-Scanner

Virenschutz mit erweiterten Automatisierungsmöglichkeiten für fortgeschrittene Anwender

Die Dr.Web Konsolen-Scanner ohne grafische Benutzeroberfläche verwenden die gemeinsame Dr.Web Virendatenbank und das gemeinsame Such-Modul. Die Konsolen-Scanner sind für MS DOS, OS/2 und Windows gedacht. Um den Virenschutz verwalten zu können, müssen Sie über ausreichende Erfahrungen mit der Kommandozeile verfügen.

Vorteile

- Minimale Systemanforderungen: Die Konsolen-Scanner laufen einwandfrei unter integrierten Systemen und können sogar leistungsschwache Computer sicher schützen
- Komfortable Prüfung: Der Administrator kann die manuelle Prüfung bzw. Prüfung nach Zeitplan durchführen
- Desinfektion der von Viren befallenen Workstations und Server (u.a. außerhalb des Netzwerks)
- Hohe Virenresistenz und Möglichkeit der Installation auf dem infizierten Computer
- Automatisierung der Routinearbeit dank vielfältigen Möglichkeiten der Kommandozeile
- Sichere Entfernung von Viren, die in der Dr.Web Virendatenbank noch nicht eingetragen sind, bzw. Viren in Archiven unbekannter Formate
- Starten von einem beliebigen Datenträger aus (CD oder USB-Speicher)

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/console/

© Doctor Web, 2016

Dr.Web Mobile Security

Schutz für mobile Endgeräte

Schutzkomponenten von Dr.Web Mobile Security

Schutzkomponenten	Android	Symbian	Windows Mobile
Antivirus	+	+	+
Antispam	+	+	+
Antitheft	+		
URL-Filter	+		

Lizenzierung für Dr.Web Mobile Security

1. Das Produkt wird nach der Anzahl der zu schützenden mobilen Endgeräte (1-5) lizenziert
2. Laufzeit: 6, 12, 24 oder 36 Monate / Laufzeit von OEM-Lizenzen: 3 oder 6 Monate
3. Für dieses Produkt sind keine Rabatte vorgesehen. Um das Produkt nach Ablauf der Lizenz weiter zu benutzen oder Ihre Lizenz zu erweitern, müssen Sie eine neue Lizenz erwerben.

Dr.Web für Android

Funktionen und Vorteile

- Schnelle und vollständige Prüfung des gesamten Dateisystems oder einzelner Dateien und Verzeichnisse auf Anforderung des Benutzers
- Dateiüberprüfung in Echtzeit durch SpIDer Guard
- Erkennung von neuen und böswilligen Programmen durch Origins Tracing™
- Schutz der SD-Karte gegen Infektion durch Autostart-Dateien und Exploit.Cpllnk, die eine Gefahr für Windows-Rechner darstellen
- Verschiebung entdeckter Schädlinge in die Quarantäne mit der Option auf Wiederherstellung
- Minimale Systembelastung
- Schonung der Akku-Laufzeit
- Geringes Internetvolumen durch kleine Updates der Virendatenbanken
- Ausführliche Statistiken
- Intuitive Bedienung der Anwendung

Antispam

Schützt Sie vor unerwünschten Anrufen und SMS-Nachrichten.

- Verschiedene Filtermodi für Anrufe und SMS-Nachrichten
- Eigene Filterprofile erstellen
- Eigene Blacklist erstellen
- Gesperrte Anrufe und SMS-Nachrichten einsehen

© Doctor Web, 2016

Diebstahlschutz

Diese Komponente hilft Ihnen, Ihr mobiles Endgerät bei Verlust oder Diebstahl zu finden und vertrauliche Daten zu löschen.

- Sperrung Ihres mobilen Endgeräts nach einem Neustart
- Sperrung Ihres mobilen Endgeräts mit der Aufforderung zur Passworteingabe (die Zahl der Versuche ist begrenzt)
- Entsperrung via SMS
- Abruf von GPS-Informationen Ihres Endgerätes als Link auf Google Maps
- Löschen der im Telefon und auf der SD-Karte gespeicherten Daten per Fernzugriff
- Einschalten des Sounds und Sperrung des Bildschirms
- Angabe des Textes, der auf dem Bildschirm Ihres Endgerätes angezeigt werden soll
- Erstellen einer Liste von Telefonnummern Ihrer Freunde und Verwandten, die eine Nachricht über den Wechsel Ihrer SIM-Karte auf dem verlorenen Endgerät erhalten sollen. Mit diesen Nummern können Sie die Diebstahlschutz-Komponente verwalten, falls Sie das Passwort zur Entsperrung vergessen haben.

URL-Filter Cloud Checker

Der Cloud Checker soll den Zugriff auf unerwünschte Web-Inhalte blockieren. Folgende Kategorien der Web-Inhalte werden blockiert:

- Drogen
- Bekannte Virenquellen
- Schimpfwörter
- Terrorismus
- Gewalt
- Waffen
- Webseiten für Erwachsene

© Doctor Web, 2016

Dr.Web Enterprise Security Suite: Produkte für Business

Dr.Web Enterprise Security Suite ist ein Gesamtpaket von Dr.Web Produkten, die sämtliche Schutzwerkzeuge für alle Computer Ihres Unternehmensnetzwerks und ein einheitliches Verwaltungscenter für die meisten Computer enthalten.

Die Produkte sind je nach geschütztem Objekt in 5 Gruppen aufgeteilt. Dies erleichtert die Suche nach einem passenden Produkt.

Kommerzielles Produkt	Software-Produkt
Dr.Web® Desktop Security Suite Schutz für Workstations, Clients der Terminalserver, der virtuellen Server und integrierten Systeme	Dr.Web® für Windows
	Dr.Web® für Linux
	Dr.Web® für OS X
	Dr.Web® für MS DOS*
	Dr.Web® für OS/2*
Dr.Web® Server Security Suite Schutz für Datei- und Anwendungsserver (u.a. virtuelle Server und Terminalserver)	Dr.Web® für Server Windows
	Dr.Web® für Server UNIX
	Dr.Web® für OS X Server
	Dr.Web® für Server Novell NetWare
Dr.Web® Mail Security Suite E-Mail-Schutz	Dr.Web® für Mailserver und Gateways UNIX
	Dr.Web® für MS Exchange
	Dr.Web® für IBM Lotus Domino für Windows
	Dr.Web® für IBM Lotus Domino für Linux
	Dr.Web® für Mailserver Kerio für Windows
	Dr.Web® für Mailserver Kerio für Linux
	Dr.Web® für Mailserver Kerio für OS X
Dr.Web® Gateway Security Suite Schutz für Gateways (SMTP- und Internet-Gateways)	Dr.Web® für Internet-Gateways UNIX
	Dr.Web® für Internet-Gateways Kerio
	Dr.Web® für MIMEsweeper*
	Dr.Web® für Qbik WinGate*
	Dr.Web® für Microsoft ISA Server und Forefront TMG*
Dr.Web® Mobile Security Suite Schutz für mobile Endgeräte	Dr.Web® für Windows Mobile
	Dr.Web® für Symbian OS*
	Dr.Web® für Android

* Ohne Verwaltungscenter

© Doctor Web, 2016

Produktwahl

1. Was muss geschützt werden?	2. Unter welchem Betriebssystem funktionieren die zu schützenden Endgeräte?*	3. Brauchen Sie nur den Virenschutz oder den Rundumschutz?	4. Brauchen Sie einen Kryptograph?	5. Wieviele Objekte müssen geschützt werden?	6. Welche Laufzeit soll eine Lizenz haben?	7. Ist dies der Erstkauf, die Verlängerung, der Zukauf oder Zukauf und Verlängerung? Hat der Kunde das Recht für einen Preisvorteil?
Produkt	Betriebssystem/ Plattform	Basislizenz	Zusätzliche Schutzkomponenten	Lizenzzahl	Lizenzlaufzeit	Lizenztyp und eventuelle Prreisvorteile
Workstations (Dr.Web Desktop Security Suite)	■ Windows XP/2003/ Vista/2008/ 7/8/2012/ 10 (32 und 64 Bit)	■ Rundumschutz ■ Antivirus	■ Verwaltungscenter	1....	12, 24 oder 36 Monate	
	■ OS X ■ Linux	■ Antivirus	■ Verwaltungscenter			
	MS DOS, OS/2					
Dateiserver (Dr.Web Server Security Suite)	■ Windows ■ OS X Server ■ UNIX	■ Antivirus	■ Verwaltungscenter	1...		
E-Mail-Verkehr (Dr.Web Mail Security Suite)	■ UNIX ■ MS Exchange ■ Lotus Domino ■ Kerio	■ Antivirus	■ Antispam ■ SMTP-Proxy ■ Verwaltungscenter	■ Unbeschränkte Anzahl von Anwendern ■ Server – mit bis zu 3 000 zu schützenden Anwendern		
Internetverkehr (Dr.Web Gateway Security Suite)	■ Internet-Gateways Kerio ■ E-Mail-Gateways UNIX	■ Antivirus	■ Verwaltungscenter	■ Unbeschränkte Anzahl von Anwendern		
	■ Qubik WinGate ■ MIMEsweeper ■ Dr.Web für Microsoft ISA Server und Forefront TMG		■ Antispam	■ Server – mit bis zu 3 000 zu schützenden Anwendern		
Mobile Endgeräte (Dr.Web Mobile Security Suite)	■ Android ■ Windows Mobile	■ Rundumschutz	■ Verwaltungscenter	Unbeschänkte Anzahl von mobilen Endgeäten		
	■ Symbian					
Jetzt haben Sie alle nötigen Daten für die Kalkulation des Preises Ihrer Lizenz.						

* Dieser Schritt ist wichtig bei der Auswahl des Schutzes für Workstations, weil das Paket von zusätzlichen Komponenten vom verwendeten Betriebssystem abhängt (siehe Lizenzierung)

© Doctor Web, 2016

Dr.Web Verwaltungscenter

Zentral verwaltbarer Schutz für alle Computer Ihres Unternehmensnetzwerks

Schlüsselfunktionen

Zentrale Verwaltung aller Schutzkomponenten, Überwachung geschützter Computer und Konfiguration einer automatischen Reaktion auf Viren-Ereignisse.

Vorteile

- Geringe Kosten bei der Verwaltung des Schutzsystems für das Unternehmensnetzwerk aus einer beliebigen Region der Welt von einem Arbeitsplatz aus (Web-Administration)
- Minimale Gesamtkosten im Vergleich zu Konkurrenzprogrammen durch die Möglichkeit der Einrichtung des Netzwerks unter Windows- und UNIX-Servern, leichte Installation und sicherer Schutz
- Das Schutzsystem kann unabhängig von der Größe und den Besonderheiten (Anzahl von Mitarbeitern, Filialen, Topologie, Active Directory Server vorhanden/nicht vorhanden) in einem beliebigen Unternehmensnetzwerk eingerichtet werden
- Möglichkeit der Einrichtung von Agenten auf Workstations durch Active Directory, Start-Skripts oder Remote-Installation. Die Installation ist möglich, selbst wenn ein Computer für den Antivirus-Server nicht erreichbar ist.
- Einstellung individueller sicherheitspolitischer Vorgaben für Unternehmen und einzelne Mitarbeitergruppen
- Automatisierung durch die Integration mit Windows NAP
- Ausschließliche Skalierbarkeit für Netzwerke beliebiger Größe und Komplexität durch die Hierarchie interagierender Antivirus-Server des Verwaltungscenters und eines separaten SQL-Servers für die Datenlagerung sowie durch die Interaktion zwischen den oben genannten Komponenten und geschützten Objekten des Netzwerks
- Unterstützung mehrerer Protokolle für den Datenaustausch zwischen Computern und dem Antivirus-Server: TCP/IP (einschließlich IPV6), IPX/SPX und NetBIOS
- Sichere Datenübertragung zwischen Systemkomponenten durch die Möglichkeit der Verschlüsselung
- Minimaler Netzwerk-Verkehr: Für die Datenkompression zwischen Client und Server sorgt das auf TCP/IP, IPX/SPX oder NetBIOS basierende Protokoll
- Das Protokoll für Aktionen des Administrators ermöglicht das Verfolgen aller Installations- und Konfigurationsschritte im System und sorgt für Transparenz. Alle Komponenten des Systems können Aktionen mit einer benutzerdefinierten Detailtiefe protokollieren.
- Komfortable Benachrichtigung des Administrators über eventuelle Probleme im Antivirus-Netzwerk
- Möglichkeit der Zuordnung von Administratoren für verschiedene Gruppen. So kann das Verwaltungscenter in Unternehmen mit höheren Sicherheitsanforderungen und Unternehmen mit einer verzweigten Filialstruktur verwendet werden.
- Die Konfiguration von sicherheitspolitischen Vorgaben für verschiedene Benutzertypen (u.a. mobile Benutzer) und Workstations trägt zum aktuellen Stand des Schutzsystems bei
- Selbständige Anpassung der Schutzparameter ist aus Sicherheitsgründen unmöglich
- Schutz für Netzwerke ohne Internetverbindung

© Doctor Web, 2016

- Verwendung der meisten am Markt vorhandenen Datenbanken: Dr.Web Enterprise Suite ist sowohl mit der internen als auch externen Datenbank kompatibel. Als externe Datenbank kann Oracle, PostgreSQL, Microsoft SQL Server oder Microsoft SQL Server Compact Edition sowie ein beliebiges Datenbankmanagementsystem mit der Unterstützung von SQL-92 über ODBC auftreten.
- Selbständige Erstellung von Ereignis-Bearbeitern in einer beliebigen Skriptsprache. Dies ermöglicht einen direkten Zugriff auf interne Oberflächen des Verwaltungscenters.
- Zurücksetzen von Updates, auch wenn der Update-Vorgang einen Fehler hervorruft. Der Netzwerk-Knoten wird trotzdem geschützt sein.
- Der Systemadministrator kann zusätzliche Produkte anderer Hersteller installieren und synchronisieren, was die Kosten für die Einrichtung eines Sicherheitssystems wesentlich verringert
- Übersichtliche Kontrolle der Sicherheitslage und effiziente Suche nach Workstations im Netzwerk
- Erstellung der Liste der zu aktualisierenden Produkt-Komponenten und Kontrolle des Umstiegs auf neue Versionen. Dadurch kann der Administrator notwendige und geprüfte Updates verbreiten.

© Doctor Web, 2016

Dr.Web Desktop Security Suite

Virenschutz für Workstations, Clients der Terminalserver und integrierte Systeme

- Dr.Web für Windows
- Dr.Web für Linux
- Dr.Web für OS X
- Dr.Web Konsolen-Scanner für Windows, MS DOS, OS/2

Unterstützte Betriebssysteme

Dr.Web für Windows	Dr.Web für Linux	Dr.Web für OS X	Dr.Web Konsolen-Scanner
Windows XP/2003/ Vista/2008/7/8/2012/ 10 (32 und 64 Bit)	GNU/Linux- Installationsdateien unter Intel x86/amd64 auf Baisis der Engine 2.6.37 (und höher) mit der glibc-Bibliothek 2.13 (und höher)	OS X 10.7 und höher	Windows, MS DOS, OS/2

Lizenzierung von Dr.Web Desktop Security Suite

Die Lizenzierung richtet sich nach der Anzahl an Workstations und Clients, die mit dem Terminalserver oder Clients integrierter Systeme verbunden werden.

Die Software-Produkte der Gruppe Dr.Web Desktop Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im letzten Fall wird das Verwaltungscenter von Dr.Web Enterprise Security Suite (Dr.Web Konsolen-Scanner exkl.), die Firewall und der Kryptograph (nur für Dr.Web für Windows) lizenziert.

Lizenzoptionen

	Windows Windows 10/8/7/ Vista/XP	**Windows** 8/7/Vista/XP SP2/ 2000 SP4 + Rollup 1	**Linux**	**OS X**	**MS DOS, OS/2**
Basislizenz	Rundumschutz	Antivirus Windows 8/7/Vista/XP SP2/2000 SP4 + Rollup 1 (32 und 64 Bit)			
Schutzkomponente der Basislizenz	■ Antivirus ■ Antispyware ■ Antirootkit ■ Antispam ■ Web-Antivirus ■ Office Control ■ Firewall	■ Antivirus ■ Antispyware ■ Antirootkit ■ Firewall	■ Antivirus ■ Antispyware	■ Antivirus ■ Antispyware ■ Antirootkit	■ Antivirus ■ Antispyware ■ Antirootkit
Zusätzliche Schutzkomponenten					
Verwaltungscenter	+	+	+	+	–

Die Produkte der Gruppe Dr.Web Desktop Security Suite (Konsolen-Scanner exkl.) sind auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

© Doctor Web, 2016

Dr.Web Server Security Suite

Schutz für Datei- und Anwendungsserver (u.a. virtuelle Server und Terminalserver)

- Dr.Web für Server Windows
- Dr.Web für Server Novell NetWare
- Dr.Web für OS X Server
- Dr.Web für Server UNIX (Samba)

Unterstützte Betriebssysteme

Dr.Web für Server Windows	Dr.Web für Server UNIX	Dr.Web für Server Novell NetWare	Dr.Web für OS X Server
Microsoft Windows Server 2000* / 2003 (x32 & x64*) / 2008 / 2012 (x64)	■ Linux mit Kernel 2.4.x und höher ■ FreeBSD 6.x und höher für Plattform Intel x86 und amd64 ■ Solaris 10 für Plattform Intel x86 und amd64	Novell NetWare 4.11–6.5	OS X Server 10.7 (32 und 64 Bit)

* Unterstützung nur für Version 7.0

Die Software-Produkte der Gruppe Dr.Web Server Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden.

Dr.Web für Server Windows	Dr.Web für Server UNIX	Dr.Web für Server Novell NetWare	Dr.Web für OS X Server
Basislizenz: Antivirus			
Zusätzliche Schutzkomponenten: Verwaltungscenter			
+	+	+	+

Die Software-Produkte der Gruppe Dr.Web Server Security Suite sind auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

Dr.Web für Server Windows

Virenschutz für Datei- und Terminalserver unter Windows (u.a. Anwendungsserver)

Vorteile

- Möglichkeit der Verwendung in Unternehmen, in denen ein höheres Sicherheitsniveau erforderlich ist (das Produkt entspricht den Anforderungen des russischen Rechts und verfügt über zahlreiche Konformitätszertifikate vom Föderalen Dienst für technische Kontrolle und Föderalen Sicherheitsdienst)
- Hohe Leistungsfähigkeit und Funktionsstabilität
- Hoher Durchsatz des Scanners bei minimaler Auslastung des Betriebssystems. Dr.Web kann deshalb auf Servern beliebiger Konfiguration einwandfrei funktionieren.
- Reibungslose Funktion des Antivirenprogramms im automatischen Modus

© Doctor Web, 2016

- Flexible Verteilung der Auslastung des Dateisystems durch die vorgeschobene Prüfung von Dateien, die nur im Lesen-Modus geöffnet werden
- Flexibles und clientorientiertes Konfigurationssystem (Auswahl des zu prüfenden Objektes und der Aktion für entdeckte Viren oder verdächtige Dateien)
- Leichte Installation und Administration
- Sofortschutz nach der Installation (mit Default-Einstellungen)
- Transparenz (Protokolle mit benutzerdefinierter Detailtiefe)

Schlüsselfunktionen

- Prüfung von Serverbänden nach Zeitplan oder auf Anforderung des Administrators
- Prüfung „on the fly" während der Speicherung oder Öffnung von Dateien auf dem Server von Workstations aus
- Mehrströmige Prüfung
- Automatische Trennung der Verbindung vom Server der Workstations (Quelle einer Virenbedrohung)
- Blitzschnelle Benachrichtigung des Administrators, anderer Benutzer und Benutzergruppen über Virenereignisse via E-Mail oder SMS
- Verschiebung infizierter Dateien in die Quarantäne
- Desinfektion, Wiederherstellung und/oder Löschung der in der Quarantäne befindlichen Dateien
- Protokollierung von Aktionen des Programms
- Automatisches Update der Virendatenbanken
- Beseitigung von Bedrohungen bereits während der Installation
- Schonende Systemanforderungen und Berücksichtigung der Systemleistung
- Maximaler Scan-Durchsatz durch die mehrströmige Virenprüfung und Verteilung der Serverauslastung
- Automatische Wiederherstellung von Produktkomponenten aus dem lokalen Registry
- Neues System für die Benachrichtigung von Benutzern ohne Ablenkungsnachrichten*
- Dr.Web Cloud: Blitzschnelle Reaktion auf neueste Bedrohungen*
- Proaktiver Virenschutz bietet einen zuverlässigen Schutz vor unbekannten Bedrohungen durch die Blockierung der Modifikation kritischer Windows-Dateien und die Überwachung von sicherheitsgefährdenden Aktionen*
- Neues System für das Hintergrund-Scannen und die Neutralisierung aktiver Bedrohungen. Dr.Web für Windows 8.0 kann trotz Widerstandes von Malware eine beliebige Bedrohung beseitigen.
- Verwaltung von Dr.Web für Windows innerhalb eines lokalen Netzwerkes durch Dr.Web Verwaltungscenter von einem beliebigen PC aus
- Verschiedene Scan-Modi (schnell/vollständig/benutzerdefiniert) für den Hauptspeicher, Laufwerke, Logical Volumes, Network Volumes, Verzeichnisse, Dateien, E-Mail-Dateien, Speicherungen auf der Festplatte und sonstige Systemobjekte

Systemanforderungen

- Prozessor, der das Kommandosystem i686 und höher unterstützt
- Betriebssystem: Microsoft Windows Server 2000**/2003 (x32 und x64**)/2008/2012 (x64)
- Hauptspeicher: 512 MB

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/fileserver/win/

* Vorhanden für Windows Server 2008 und höher

** Unterstützung nur für Version 7.0

© Doctor Web, 2016

Dr.Web Antivirus für OS X Server

Virenschutz für Server unter OS X Server

Schlüsselfunktionen

- Prüfung von Autostart-Dateien, Wechseldatenträgern, Netzwerk-Treibern und Logical Values, E-Mails sowie Dateien und Verzeichnissen (u.a. gepackt und archiviert)
- Auswahl eines Scanmodus: Schnell, vollständig und benutzerdefiniert
- Virenprüfung manuell, automatisch oder nach Zeitplan
- Passwortschutz des Wächters SpIDer Guard® vor unerlaubtem Zugriff
- Auswahl einer Aktion für infizierte, verdächtige und sonstige Objekte, einschließlich der Desinfektion, Verschiebung in die Quarantäne und der Entfernung (auch wenn die früher ausgewählte Aktion unmöglich war)
- Auslassen der Prüfung für Pfade und Dateien auf Anforderung
- Erkennung und Beseitigung von Viren, die durch unbekannte Packprogramme gepackt wurden
- Protokollierung des Zeitpunktes eines Ereignisses, des geprüften Objektes und einer Aktion
- Automatisches Update der Virendatenbanken und Programm-Module auf Anforderung oder nach Zeitplan
- Benachrichtigung (u.a. Ton-Benachrichtigung) über Virenereignisse
- Verschiebung infizierter Objekte in die Quarantäne mit der Option der Wiederherstellung und Einschränkung der Quarantäne-Größe
- Desinfektion, Wiederherstellung und Entfernung der in die Quarantäne verschobenen Objekte
- Detaillierte Protokollierung
- Verwendung von Modulen als Tools der Kommandozeile, Möglichkeit der Integration von Modulen in Apple Scripts-Systeme

Vorteile

- Komfortables Verwaltungscenter
- Hoher Scan-Durchsatz
- Möglichkeit der Erstellung eigener Scanprofile
- Sicherer Virenschutz in Echtzeit
- Minimale Systemauslastung
- Geringer Internetverkehr beim Update
- Vielfältige Einstellungen
- Leichte Bedienung
- Intuitiv verständliche Benutzeroberfläche

Systemanforderungen

- OS X Server 10.7 oder höher (32 und 64 Bit)
- Prozessor Intel
- Internetverbindung (für die Registrierung und das Herunterladen von Updates)

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/fileserver/mac/

© Doctor Web, 2016

Dr.Web für Server Novell NetWare

Virenschutz für Dateiserver

Schlüsselfunktionen

- Prüfung von Serverbänden nach Zeitplan oder auf Anforderung des Administrators
- Prüfung „on the fly" sämtlicher Dateien, die durch den Server übertragen werden
- Mehrströmige Prüfung
- Regelung der Serverauslastung und Einstellung der Scanpriorität im System
- Automatische Trennung der Verbindung vom Server des PCs (Infektionsquelle)
- Protokollierung der Prüfungsergebnisse, benutzerdefinierte Detailtiefe des Protokolls
- Benachrichtigung über infizierte Objekte
- Desinfektion, Löschung oder Verschiebung infizierter Dateien in die Quarantäne
- Administration des Antivirenprogramms durch die Server-Konsole bzw. Remote-Konsole
- Sammlung von Statistiken über die Prüfung und Aktionen des Antivirenprogramms
- Automatisches Update der Virendatenbanken

Vorteile

- Unterstützte Versionen: Novell NetWare ab 4.11 bis 6.5
- Unterstützung von NetWare-Namen
- Hoher Durchsatz des Scanners bei großen Datenmengen und minimaler Auslastung des Betriebssystems
- Einfache Installation
- Flexible und clientorientierte Konfiguration (Auswahl des zu prüfenden Objektes sowie der entsprechenden Aktion für entdeckte Viren oder verdächtige Dateien)

Systemanfoderungen

- Novell NetWare 4.11-6.5 mit installierten Erweiterungen aus der Minimum Patch List

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/fileserver/novell/

© Doctor Web, 2016

Dr.Web für Server UNIX

Virenschutz für Dateiserver Unix

Vorteile

- Hohe Leistungsfähigkeit und Funktionsstabilität
- Hoher Durchsatz des Scanners bei minimaler Auslastung des Betriebssystems. Dr.Web kann deshalb auf Servern beliebiger Konfiguration einwandfrei funktionieren.
- Flexible und clientorientierte Konfiguration (Auswahl des zu prüfenden Objektes sowie der entsprechenden Aktion für entdeckte Viren oder verdächtige Dateien)
- Hervorragende Kompatibilität (Konflikte mit bekannten Firewalls und Datei-Wächtern sind ausgeschlossen)
- Unterstützung für Monitoring-Systeme (Cacti, Zabbix, Munin, Nagios usw.)
- Leichte Installation, Konfiguration und Administration

Schlüsselfunktionen

- Prüfung von Serverbänden nach Zeitplan oder auf Anforderung des Administrators
- Verbessert! Prüfung „on the fly" während der Speicherung oder Öffnung von Dateien auf dem Server von den Workstations aus
- Mehrströmige Prüfung
- Automatische Trennung der Verbindung vom Server der Workstations (Quelle einer Virenbedrohung)
- Blitzschnelle Benachrichtigung des Administrators, anderer Benutzer und Benutzergruppen über Virenereignisse via E-Mail oder SMS
- Verbessert! Verschiebung infizierter Dateien in die Quarantäne
- Desinfektion, Wiederherstellung und/oder Löschung der in der Quarantäne befindlichen Dateien
- Protokollierung von Aktionen des Programms
- Automatisches Update der Virendatenbanken

Unterstützte Betriebssysteme

- GNU/Linux (Kernel ab 2.6.37 und Bibliothek glibc 2.13 und höher);
- FreeBSD;
- Solaris — nur für Intel x86/amd64.

Die Betriebssysteme müssen den Samba-Server ab Version 3.0 und das Authentifikationsverfahren PAM verwenden.

Bei einer 64-Bit-Version soll die Unterstützung für 32-Bit-Anwendungen verfügbar sein.

HDD:

- Mind. 1 GB

Die Funktionsfähigkeit der Produktes wurde getestet auf: Debian (7.8, 8), Fedora (20, 21), Ubuntu (12.04, 14.04, 14.10, 15.04), CentOS (5.11, 6.6, 7.1), Red Hat Enterprise Linux (5.11, 6.6, 7.1), SUSE Linux Enterprise Server (11 SP3, 12), FreeBSD (9.3, 10.1), Solaris (10 u11).

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/fileserver/unix/

© Doctor Web, 2016

Dr.Web Mail Security Suite

E-Mail-Schutz

- Dr.Web für Mailserver UNIX
- Dr.Web für MS Exchange
- Dr.Web für IBM Lotus Domino (Windows, Linux)
- Dr.Web für Mailserver Kerio (Windows, Linux)

Unterstützte Betriebssysteme

Dr.Web Produkt	Windows	Linux	FreeBSD	Solaris
		Für Plattform Intel x86		
Dr.Web für Mailserver UNIX		Mit Kernel 2.4.x und höher	Version 6.x und höher	Version 10
Dr.Web für MS Exchange	Server 2000 / 2003 / 2008 / 2012			
Dr.Web für IBM Lotus Domino	Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (32 und 64 Bit)	Red Hat Enterprise Linux (RHEL) 4, 5 und 6, Novell SuSE Linux Enterprise Server (SLES) Version 9, 10 und 11 (32 Bit)		
Dr.Web für Mailserver Kerio OS X 10.7	2000/XP/Vista/7, Server 2003/2008/2012	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, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Lizenzierung

Lizenztypen

- Lizenz nach Anzahl der zu schützenden Anwender (unbeschränkt)
- Lizenz pro geschütztem Server (für die Prüfung des unbeschränkten E-Mail-Verkehrs auf einem Server mit bis zu 3 000 zu schützenden Anwendern)

Dr.Web Software-Produkte für den E-Mail-Schutz können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden.

Durch die Verwendung der Produkte für den E-Mail-Schutz und der zusätzlichen Schutzkomponente SMTP-Proxy wird nicht nur die allgemeine Sicherheitslage im Netzwerk erhöht, sondern auch die Auslastung interner Server und Workstations verringert.

© Doctor Web, 2016

Lizenzvarianten

	Dr.Web für MS Exchange	Dr.Web für IBM Lotus Domino	Dr.Web für Mailserver UNIX	Dr.Web für Mailserver Kerio
Basislizenz	Antivirus			
Zusätzliche Schutzkomponenten				
Antispam	+	+	+	
SMTP-Proxy	+	+	+	+
Verwaltungscenter	+	+	+	+

Dr.Web für den E-Mail-Schutz ist auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

Dr.Web für Mailserver UNIX

Viren- und Spamschutz für E-Mail-Verkehr auf Servern unter UNIX (Linux/FreeBSD/Solaris(x86)

Schlüsselfunktionen

- Filterung von E-Mails auf Viren und Spam
- Analyse von E-Mails und ihrer Komponenten
- Korrekte Prüfung der meisten Archivformate (einschließlich mehrbändiger und selbstextrahierender Archive)
- White- und Blacklists
- Konfigurierbare Benachrichtigung
- Sammlung von Statistiken
- Schutz von Programm-Modulen vor Ausfällen

Vorteile

Dr.Web für Mailserver UNIX verfügt über Konformitätszertifikate des Föderalen Dienstes für technische Überwachung und Exportkontrolle und des Föderalen Sicherheitsdienstes. So können Dr.Web Sicherheitsprodukte in Unternehmen mit höheren Sicherheitsanforderungen verwendet werden. Die Archivierung aller E-Mails ermöglicht auch den Einsatz des Produktes in IT-Systemen von Kreditanstalten.

Bedarfsgerechte Konfiguration

Für die Konfiguration von Dr.Web für Mailserver UNIX können verschiedene Regeln verwendet werden. Dies erhöht die Flexibilität des Produktes und unterscheidet es von Konkurrenzprodukten, für deren Konfiguration statische Parameter der Konfigurationsdatei verwendet werden. Die Filterung und Änderung von E-Mails erfolgt im Einklang mit sicherheitspolitischen Vorgaben. Dabei kann der Administrator entsprechende Bearbeitungsregeln nicht nur für verschiedene Benutzer und Gruppen, sondern auch für jede einzelne E-Mail definieren. So entspricht das Produkt beliebigen Sicherheitsanforderungen und dem Datenschutzgesetz.

© Doctor Web, 2016

Geringer Administrationsaufwand

Trotz der Vielzahl verschiedener Funktionen erfordert Dr.Web für Mailserver UNIX keine längere Einstellung vor der Einrichtung des Programms. Außerdem wird Dr.Web für Mailserver UNIX nicht nur als Software-Produkt, sondern auch inklusive in Dr.Web Office Shield (Server, der nach dem Prinzip „installieren und vergessen" funktioniert) geliefert.

Schnelle Rückmeldung

Die Technologie für die mehrströmige Prüfung sorgt für eine schnelle Rückmeldung des Systems. Die Prüfung erfolgt „on the fly". Gleichzeitig werden weitere Dateien empfangen. So können Endanwender E-Mails sekundenschnell erhalten.

Weitere Vorteile von Dr.Web Antispam

- Training ist nicht erforderlich. Im Unterschied zu Antispam-Programmen, die auf der Bayes-Analyse basieren, funktioniert Dr.Web Antispam sofort nach der Installation.
- Sprachunabhängige Spam-Erkennung
- Entsprechende Aktionen für verschiedene Spam-Kategorien
- Black- und Whitelists, die die Schädigung des Unternehmensrufes unmöglich machen
- Rekordminimum bei Erkennungsfehlern
- Update einmal pro 24 Stunden. Die Erkennung unerwünschter E-Mails basiert auf mehreren tausend Regeln. Das Herunterladen von großen und häufigen Updates ist nicht erforderlich.

Schutz vertraulicher Daten

Das Produkt kann E-Mails wiederherstellen, die zufällig gelöscht wurden, und ermöglicht die Untersuchung von Datenverlusten. Dafür sorgt auch die Möglichkeit der Quarantäne-Verwaltung sowohl über die Web-Oberfläche als auch durch ein entsprechendes Tool. Darüber hinaus werden alle durchgehenden E-Mails archiviert.

Leichte Administration

Die Verwendung der Web-Oberfläche zur Konfiguration und Verwaltung des Produktes ermöglicht eine leichte Konfiguration aus einer beliebigen Region der Welt.

Konfigurierbare Lösung

Dr.Web für Mailserver UNIX kann in Lösungen anderer Hersteller integriert werden. Durch das offene API kann das Programm um neue Funktionen erweitert werden.

Erweiterbare Funktionalität

Dr.Web für Mailserver UNIX kann leicht um weitere Funktionen erweitert werden. Jedes Plug-in ist mit allen unterstützten MTAs kompatibel.

Plug-ins

- **Dr.Web** ist ein Plug-in, das E-Mails durch Dr.Web Engine auf Viren prüft
- **Vaderetro** ist ein Plug-in, das E-Mails durch Vade Retro Bibliothek auf Spam filtert
- **Headersfilter** ist ein Plug-in, das E-Mails nach E-Mail-Köpfen filtert

© Doctor Web, 2016

Dr.Web SMTP-Proxy

Durch seine modulare Struktur kann Dr.Web für Mailserver UNIX als SMTP-Proxy (Filter, welcher E-Mails vor dem Eingang auf dem Server bearbeitet) verwendet werden

Das Modul Dr.Web SMTP-Proxy kann sowohl in der demilitarisierten Zone (DMZ) als auch im E-Mail-System installiert werden. Der Server für die Prüfung von E-Mails kann in die DMZ verlagert und der Mailserver vom Internet getrennt werden. Dadurch erhält der Übeltäter sogar im Einbruchsfall keinen Zugang zu vertraulichen Daten. Die Lösung bietet die Prüfung von E-Mails per SMTP/LMTP.

Dr.Web für Mailserver UNIX als SMTP-Proxy:

- erhöht die allgemeine Sicherheitslage im Netzwerk
- ermöglicht die Verbesserung der Datenfilterung wegen fehlender Server-Einschränkungen
- verringert die Auslastung interner Mailserver und Workstations
- erhöht die Funktionsstabilität

Vorteile

Schutz vor Spammer-Angriffen

Der Administrator kann Parameter der SMTP-Sitzung einschränken und die Wahrscheinlichkeit eines Spam-Angriffs ausschließen.

Überprüfung der IP-Adresse auf Authentizität

Dr.Web SMTP-Proxy ermöglicht es, die IP-Adresse auf ihre Authentizität zu prüfen. Dadurch wird der Anwender vor Spam-Mails, die von falschen IP-Adressen versendet werden, geschützt.

Schutz vor Hacker-Angriffen

Schutz vor Hacker-Angriffen mit Dr.Web SMTP-Proxy: Passive (PLAIN, LOGIN usw.) und aktive Angriffe.

Schutz vor Spam-Fallen

Web SMTP-Proxy ermöglicht die Überprüfung des Empfängers auf eine Spam-Falle.

Schutz vor inkorrekten E-Mails

Das Produkt blockiert E-Mails mit leeren Absenderzeilen und bearbeitet dabei inkorrekt erstellte E-Mails.

Geringer Internetverkehr

Dr.Web SMTP-Proxy ermöglicht die Einschränkung der Größe von E-Mail-Anhängen.

Einschränkung von Open Relays Servern

Wenn Sie einen solchen Server einrichten möchten, kann der Administrator durch Dr.Web SMTP-Proxy eine Liste von Domains erstellen, an die E-Mails versendet werden dürfen.

Unterstützte Betriebssysteme

- Distributionsdateien Linux mit Kernel 2.4.x und höher
- FreeBSD 6.x, 7.x, 8.x für die Plattform Intel x86
- Solaris 10 für die Plattform Intel x86
- CommuniGate Pro, Courier MTA, Exim, Postfix, QMail, Sendmail, ZMailer

Nützliche Links

Produktbeschreibung: http://new-download.drweb.com/maild

© Doctor Web, 2016

Dr.Web für MS Exchange

Viren- und Spamprüfung von Daten, die über den Server MS Exchange 2000/2003/2007/2010/2013/2016 übertragen werden

Vorteile

- Einsatz in Unternehmen mit höheren Sicherheitsanforderungen: Das Produkt verfügt über zahlreiche Konformitätszertifikate des Föderalen Dienstes für technische Überwachung und des Föderalen Sicherheitsdienstes
- Flexible Installation und bedarfsgerechte Konfiguration
- Ein hoher Durchsatz des Scanners bei minimaler Systemauslastung sorgt dafür, dass Dr.Web auf Servern beliebiger Konfiguration einwandfrei funktioniert
- Das Antispam-Modul erfordert kein Training und funktioniert sofort nach der Installation. Die Serversauslastung wird dadurch verringert und die Leistung der Mitarbeiter wesentlich erhöht.
- Filterung nach Black- und Whitelists: Bestimmte E-Mail-Adressen können von der Prüfung ausgeschlossen werden
- Filterung nach Dateitypen mit geringem Verkehrsaufwand
- Gruppierung: Für verschiedene Mitarbeitergruppen werden entsprechende Parameter definiert. Dadurch wird die Einrichtungsdauer des Virenschutzes verringert und der weitere Service vereinfacht.
- Hohe Leistung und Funktionsstabilität durch die mehrströmige Prüfung
- Einzigartige Technologien zur Entdeckung von unbekannten Packprogrammen und böswilligen Dateien
- Automatisches Starten der Anwendung (beim Systemstart)
- Bequemes Update durch den Windows-Planer
- Dokumentation mit detaillierten Informationen

Schlüsselfunktionen

- Viren- und Spamprüfung von E-Mails (einschließlich angehängter Dateien) „on the fly“
- Virenprüfung von E-Mails in Postfächern der Anwender und in allgemein zugänglichen Verzeichnissen
- Virenprüfung von Mail-Dateien, die per MS Exchange übertragen werden
- Desinfektion verseuchter Dateien
- Gruppierung von Benutzern durch ActiveDirectory
- Benutzerdefinierte Prüfung: Definieren der Maximalgröße der zu prüfenden Objekte, Auswahl von Aktionen (u.a. für Dateien, die nicht geprüft werden können) und Behandlungsmethoden für infizierte Objekte
- Erkennung und Beseitigung von böswilligen Objekten in mehrfach gepackten Dateien
- Auswahl der entsprechenden Aktion je nach Spam-Art (u.a. Verschiebung in die Quarantäne und Hinzufügen eines Präfixes in den Betreff von E-Mails)
- Hinzufügen entsprechender Hinweise in abgesendeten E-Mails
- Verschiebung infizierter und verdächtiger Dateien in die Quarantäne
- Benachrichtigung des Administrators und anderer Anwender über Virus-Ereignisse
- Automatisches Update

© Doctor Web, 2016

Systemanforderungen

Für Microsoft Exchange Server 2000/2003:

- Pentium 133 MHz (733 MHz empfohlen)
- Hauptspeicher: 256 MB (512 MB empfohlen)
- HDD: 512 MB
- Microsoft® Windows® 2000 Server oder Advanced Server mit SP4; Microsoft® Windows Server® 2003 (Standard, Enterprise oder Datacenter) mit SP1 oder höher

Für Microsoft Exchange Server 2007/2010:

- Intel mit der x64-Architektur und der Unterstützung für Intel 64 oder AMD mit der Unterstützung für AMD64
- Hauptspeicher: 2 GB
- HDD: 512 MB
- Microsoft® Windows Server® 2003 R2 x64 mit SP2; Microsoft® Windows Server® 2008 x64

Für Microsoft Exchange Server 2013/2016:

- Intel mit der x64-Architektur und der Unterstützung für Intel 64 oder AMD mit der Unterstützung für AMD64
- Hauptspeicher: 4 GB
- HDD: 1 GB
- Microsoft® Windows® Server 2008 R2; Microsoft® Windows® Server 2012; Microsoft® Windows® Server 2012 R2

Nützliche Links:

Produktbeschreibung: http://products.drweb.com/exchange/

Dr.Web für IBM Lotus Domino

Viren- und Spamschutz für IBM Lotus Domino unter Windows und Linux

Vorteile

- **Minimale Gesamtkosten**

Dr.Web für IBM Lotus Domino kann nicht nur auf einzelnen Servern, sondern auch auf Partitionsservern und Lotus Domino Clustern funktionieren. Dabei laufen Kopien der Antivirenprogramme im PC-Speicher autonom, indem sie gemeinsame Datenbanken und ausführbare Dateien verwenden. In diesem Fall muss man nur eine Kopie lizenzieren, was die Kosten für den Antivirenschutz wesentlich verringert.

- **Ready for IBM Lotus Software**

Dr.Web für IBM Lotus Domino ist im IBM Lotus Business Solutions Catalog eingetragen und verfügt über die Auszeichnung **Ready for IBM Lotus Software**. Dies belegt die Kompatibilität des Produktes mit Lotus Domino und zeugt von erfüllten IBM-Anforderungen.

- **Hohe Scangeschwindigkeit**

Der Systemaufbau von **Dr.Web für IBM Lotus Domino**, eine besondere Prüfungsmethode und eine flexible Verwaltung dieser Vorgänge ermöglichen eine hohe Scangeschwindigkeit bei minimalen Systemanforderungen. Durch die Funktion der mehrströmigen Prüfung kann das Antivirenprogramm einen großen Umfang von E-Mails gleichzeitig bearbeiten. Dadurch kann **Dr.Web für IBM Lotus Domino** einwandfrei auf Mailservern beliebiger Konfiguration funktionieren.

- **Leichte Installation und flexible Konfiguration**

Die Einrichtung von **Dr.Web für IBM Lotus Domino** kann leicht automatisiert werden. Es unterstützt Administrationsskripts und verfügt über die entsprechende Dokumentation. Eine flexible Konfiguration der Aktionsalgorithmen des Antivirenprogramms bei Scanergebnissen ermöglicht die Benachrichtigung des Absenders, Empfängers und Systemadministrators über entdeckte Viren. E-Mail-Köpfe und angehängte Dateien bleiben dabei erhalten.

© Doctor Web, 2016

Bequeme Administration

Die Gruppierung und die Verwaltung von Gruppen vereinfachen die Administration des Virenschutzes. Für jede Gruppe können verschiedene Einstellungen definiert werden. Dieselben Einstellungen können auch für mehrere Gruppen definiert werden.

Schlüsselfunktionen

- Prüfung und Filterung von E-Mails auf Viren, Spam und unerwünschte E-Mails auf Anforderung des Administrators „on the fly"
- Spam-Filterung von E-Mails (u.a. anhand von Black- und Whitelists)
- Virenprüfung von Dateien in nsf-Datenbanken
- Prüfung von Objekten auf Anfoderung durch den manuellen Start oder das Abbrechen von Aufgaben des Scanners
- Analyse von E-Mails und Sortierung aller E-Mail-Komponenten zur weiteren Analyse
- Desinfektion verseuchter E-Mails und angehängter Dateien
- Erkennung und Beseitigung von Malware in mehrfach gepackten Dateien
- Entdeckung von böswilligen Objekten, die durch unbekannte Packprogramme versteckt wurden
- Entdeckung unbekannter böswilliger Objekte
- Verschiebung infizierter und verdächtiger Objekte in die Quarantäne (der Zugriff auf die in die Quarantäne verschobenen Objekte erfolgt über das Lotus Notes Client)
- Benachrichtigung über Scanergebnisse durch Templates, die im System beschrieben sind. Dadurch können Empfänger und Administratoren entsprechende Informationen leicht und bequem erhalten.
- Erhebung von Statistiken
- Schutz vor Evasions-Techniken
- Automatisches Update

Unterstützte Betriebssysteme

Version für Windows

- Betriebssystem: Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (32 und 64 Bit).
- Lotus Domino R6.0 und höher (32 und 64 Bit).
- Prozessor Intel Pentium 133 und höher.
- RAM: 128 MB (512 MB empfehlenswert).
- HDD: 128 MB.

Version für Linux

- Betriebssystem: Red Hat Enterprise Linux (RHEL) 4 und 5, Novell SuSE Linux Enterprise Server (SLES) 9 und 10 (nur 32 Bit).
- Lotus Domino 7.x oder 8.x.
- Lotus Notes 6.5 (oder älter) für Windows.
- Prozessor Intel Pentium 133 und höher.
- RAM 64 MB (128 MB empfehlenswert).
- HDD: 90 MB.

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/lotus/

© Doctor Web, 2016

Dr.Web für Mailserver Kerio

Virenprüfung von E-Mail-Anhängen, die per SMTP/POP3 übertragen werden

Vorteile

- Hervorragende Kompatibilität mit Mailservern Kerio, die durch Kerio Technologies belegt wurde
- Möglichkeit der Arbeit im zentral verwalteten Schutzmodus dank dem Verwaltungscenter von Dr.Web Enterprise Security Suite
- Dr.Web ist zur Zeit ein einziges Antivirus-Plug-in für Mailserver Kerio
- Technischer Support
- Minimale Zustellungszeit von E-Mails und hohe Zuverlässigkeit des Produktes durch die Technologie der mehrströmigen Prüfung
- Minimale Systemanforderungen und keine Auslastung des lokalen Netzwerks
- Flexible und clientorientierte Konfiguration: Auswahl der zu prüfenden Objekte und entsprechenden Aktionen für entdeckte Viren oder verdächtige Dateien
- Auswahl der Aktionen für Dateien, die nicht geprüft werden können
- Bequeme Verwaltung über die Verwaltungskonsole des Mailservers Kerio

Schlüsselfunktionen

- Prüfung von Anhängen aller ein- und ausgehenden E-Mails

Unterstützte Betriebssysteme

Version für Windows

- HDD: mind. 350 MB
- Betriebssystem: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/2012 (32 und 64 Bit)
- Mailserver: Kerio MailServer 6.2 oder höher, Kerio Connect 7.0.0 oder höher.

Version für Linux

- HDD: mind. 290 MB
- Betriebssystem: 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 und 11.1; CentOS Linux 5.2 und 5.3; Debian 5.0; Ubuntu 8.04 LTS.
- Mailserver: Kerio MailServer 6.2 oder höher, Kerio Connect 7.0.0 oder höher.

Version für OS X

- HDD: mind. 55 MB
- Betriebssystem: OS X 10.7 und höher.
- Mailserver: Kerio MailServer 6.2 oder höher, Kerio Connect 7.0.0 oder höher.

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/mailserver/kerio/

© Doctor Web, 2016

Dr.Web Gateway Security Suite

Viren- und Spamschutz für E-Mail- und Internet-Gateways

- Dr.Web für Internet-Gateways UNIX
- Dr.Web für Internet-Gateways Kerio
- Dr.Web für MIMEswepper
- Dr.Web für Qbik WinGate

Unterstützte Betriebssysteme

	Windows	Linux	FreeBSD	Solaris
		für Plattform Intel x86 und amd64		
Dr.Web für Internet-Gateways UNIX		Kernel 2.4.x und höher	Version 6.x und höher	Version 10
Dr.Web für Internet-Gateways Kerio	2000 / XP / Vista /2003 / 2008 / 7			
Dr.Web für MIMEsweeper	2000 Server SP4 oder höher/Server 2003 / 2008 / 2008 R2 (32 und 64 Bit)			
Dr.Web für Qbik WinGate	Vista / Server 2008 / Server 2003 / XP / 2000 (32 und 64 Bit)			
MS ISA Server & Forefront TMG				

Lizenzierung

Lizenztypen

- Lizenz nach Anzahl der zu schützenden Anwender (unbeschränkt)
- Lizenz pro geschütztem Server (für die Prüfung des unbeschränkten Verkehrs auf einem Server mit bis zu 3 000 zu schützenden Anwendern)

Dr.Web Softwareprodukte für Gateways können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im letzten Fall wird auch das Verwaltungscenter von Dr.Web Enterprise Security Suite (dies gilt nur für Dr.Web für Internet-Gateways Kerio) und Antispam (außer Internet-Gateways UNIX und Kerio) lizenziert.

Lizenzvarianten

	Dr.Web für Internet-Gateways UNIX	Dr.Web für Internet-Gateways Kerio	Dr.Web für MIMEsweeper	Dr.Web für Qbik WinGate	MS ISA Server & Forefront TMG
Basislizenz	Antivirus				
Zusätzliche Schutzkomponenten					
Antispam			+	+	
Verwaltungscenter		+			

Dr.Web für Gateways ist auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

© Doctor Web, 2016

Dr.Web für Internet-Gateways UNIX

Virenprüfung von Daten, die per HTTP und FTP über das Internet-Gateway des Unternehmens (Proxy-Server) übertragen werden

Schlüsselfunktionen

- Virenprüfung der per FTP und HTTP übertragenen Daten
- Zentrale Verwaltung über das Web-Administrationstool des Verwaltungscenters von Dr.Web Enterprise Security Suite
- Zugriffsverwaltung nach MIME-Typ, Dateigröße oder Hostnamen
- Zugriffsverwaltung auf Web-Inhalte
- Optimierung der Traffic-Überprüfung via Preview
- Unterstützung der IPv4- und IPv6-Protokolle
- Prüfung und Durchführung verschiedener Aktionen je nach geprüften Dateien
- Verschiebung infizierter Dateien in die Quarantäne
- Benutzerfreundliche Protokollierung
- Zentrale Verwaltung der Server-Konfigurationen und Protokollierung
- Bearbeitung mehrerer Anfragen während einer Sitzung
- Schutz vor unerlaubtem Zugriff
- Überwachung und automatische Wiederherstellung der Systemfunktion
- Benachrichtigung des Benutzers über das Hochladen einer Malware-Webseite oder einen Virenfund

Vorteile

- Effiziente Filterung des Traffics auf Ebene des ICAP-Servers (ohne Verlangsamung der Übertragung der Web-Inhalte)
- Effizienter Schutz vor Malware beliebiger Art
- Hohe Skalierbarkeit
- Bearbeitung von großen Datenmengen in Echtzeit
- Senkung von Internetkosten
- Hervorragende Kompatibilität: Integration mit beliebiger Software, die das ICAP-Protokoll unterstützt, mit allen am Markt vorhandenen Firewalls
- Unterstützung der meisten am Markt vorhandenen UNIX-basierten Betriebssystemen
- Geringe Systemanforderungen
- Flexible und komfortable Administration

Unterstützte Betriebssysteme

- Linux mit Kernel ab 2.4.x
- FreeBSD ab 6.x (für Intel x86-Plattform und amd64)
- Solaris 10 (für Intel x86-Plattform und amd64)

Beliebige Proxy-Server, die das ICAP-Protokoll unterstützen, und zwar:

- Squid ab 3.0
- SafeSquid ab 3.0

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/gateway/unix/

© Doctor Web, 2016

Dr.Web für Internet-Gateways Kerio

Virenprüfung von Daten, die per HTTP, FTP, SMTP, POP3 und Kerio Clientless SSL VPN übertragen werden

Dr.Web für Internet-Gateways Kerio ist ein Antivirus-Plug-in, das zur Firewall Kerio angeschlossen wird. Das Plug-in wird auf dem Computer mit Kerio installiert und wird von Kerio als externe Antivirensoftware verwendet.

Vorteile

- Zuverlässiger Schutz für den Internetzugang von Privatanwendern und Unternehmen beliebiger Größe
- Leichte Administration (Möglichkeit, über alle Virenereignisse via E-Mail oder SMS benachrichtigt zu werden)
- Minimale Zustellungszeit der E-Mails durch die mehrströmige Prüfung
- Möglichkeit der Arbeit im zentral verwalteten Schutzmodus dank dem Verwaltungscenter von Dr.Web Enterprise Security Suite
- Einsehen von Funktions-Statistiken des Programms durch Web-Konsole
- Versand von Benachrichtigungen über die vom Benutzer ausgewählten Ereignisse

Schlüsselfunktionen

- Erkennung und Beseitigung von böswilligen Objekten, die via HTTP, FTP, SMTP, POP3 und Kerio Clientless SSL VPN übertragen werden
- Erkennung und Beseitigung infizierter E-Mail-Anhänge vor der Bearbeitung durch den Mailserver
- Erstellung einer Liste der zu prüfenden Datenaustauschprotokolle
- Benutzerdefinierte Prüfung: Einstellbare Maximalgröße und Typ der zu prüfenden Objekte und Auswahl von Bearbeitungsmethoden für infizierte Dateien
- Durchführung von Aktionen gegen entdeckte Bedrohungen nach Kerio-Einstellungen
- Aktivierung/Deaktivierung der Erkennung und Beseitigung von Malware bestimmter Arten
- Protokollierung von Fehlern und Ereignissen im Ereignis- und Textprotokoll
- Automatisches Update der Virendatenbanken

Systemanforderungen

Version für Windows:

- HDD: Mind. 350 MB
- Microsoft Windows 2000 SP4 + Rollup1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32 und 64 Bit)
- Kerio WinRoute Firewall 6.2 oder höher, Kerio Control 7.0.0 oder höher

Version für Kerio Control VMware Virtual Appliance und Kerio Control Software Appliance:

- HDD: Mind. 290 MB
- Kerio Control VMware Virtual Appliance oder Kerio Control Software Appliance
- Kerio Control 8.x oder höher

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/gateway/kerio/

© Doctor Web, 2016

Dr.Web für MIMEsweeper

Viren- und Spamschutz für Daten, die durch Datenfilterungsserver ClearSwift MIMEsweeper Server übertragen werden

Vorteile

Einfachheit bei der Installation und Einstellung

Die in Dr.Web für MIMEsweeper integrierten Konfigurationswerkzeuge (Programme, die Szenarien erstellen) ermöglichen die Erstellung möglichst aktueller Szenarien der E-Mail-Prüfung (Typ 1 nach der Klassifikation von ClearSwift). Je nach Einstellungen des Szenarios können Überprüfungsmeldungen sowie Meldungen über die vom Plug-in durchgeführten Aktionen in den E-Mail-Kopf und E-Mail-Körper vom Content-Filter eingefügt werden.

Flexible Einstellungen

Bei der Erkennung und Beseitigung eines infizierten Objektes versucht das Plug-in dieses Objekt zu desinfizieren oder entfernt es sofort, wenn die Desinfektionsoption nicht aktiviert ist. Wenn sich im E-Mail-Anhang einige Dateien oder Archive befinden, desinfiziert das Plug-in nur infizierte Anhänge. Bei Virenfund im E-Mail-Körper verschiebt der Content-Filter diese E-Mail in die Quarantäne. Saubere E-Mails, Dateien und Archive werden dem Empfänger ohne Änderungen zugestellt. E-Mails, die das Dr.Web Plug-in nicht neutralisieren kann, werden als Viren markiert und nach den Voreinstellungen in die Quarantäne verschoben.

DEP–Kompatibilität

Dr.Web für MIMEsweeper unterstützt die DEP-Technologie (Data Execution Prevention), die die zusätzliche Überprüfung des Speicherinhaltes ermöglicht und den Start des Schadcodes unterbindet. Dadurch brauchen die Anwender den DEP-Funktionsmodus nicht zu ändern. Die Malware kann den Mechanismus für die Bearbeitung der in Windows vorhandenen Ausnahmen nicht ausnutzen.

Schlüsselfunktionen

- Prüfung von E-Mails und Anhängen einschließlich Archiven vor der Bearbeitung durch den Mailserver
- Desinfektion infizierter Objekte
- Verschiebung infizierter und verdächtiger Dateien in die Quarantäne
- Filterung von E-Mails auf Spam (u.a. aufgrund White- und Blacklists)
- Sammlung von Statistiken
- Automatisches Update

Systemanforderungen

- Windows 2000 Server mit SP4 oder höher oder Windows Server 2003 /2008 / 2008R2
- E-Mail-Filter ClearSwift MIMEsweeper™ für SMTP 5.2 oder höher

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/mimesweeper/

© Doctor Web, 2016

Dr.Web für Qbik WinGate

Viren- und Spamschutz für Daten, die per HTTP/POP3/FTP-Protokolle des Proxy-Servers und SMTP-Servers Qbik WinGate übertragen werden

Schlüsselfunktionen

- Viren- und Spamprüfung von E-Mails, die per SMTP und POP3 übertragen werden (einschließlich angehängter Dateien)
- Virenprüfung von Dateien und Daten, die per HTTP und FTP übertragen werden
- Desinfektion von infizierten Dateien, die per HTTP übertragen werden
- Ereignis-Protokoll
- Eigene Verwaltungsoberfläche und Quarantäne-Management
- Automatisches Update der Virendatenbanken

Vorteile

- Dr.Web für Qbik WinGate verfügt über die entsprechende Dokumentation und bietet den technischen Support vom Hersteller
- Im Unterschied zu Konkurrenzprogrammen verfügt Dr.Web außerdem über die Möglichkeit der Spam-Filterung. Ein effizientes und kompaktes Antispam-Modul benötigt kein Training und ermöglicht es Ihnen, verschiedene Aktionen für jede Spam-Kategorie zu definieren sowie Black- und Whitelists zu erstellen.
- Die Technologie Origins Tracing™ sorgt dafür, dass die noch nicht eingetragenen Bedrohungen (u.a. in Archiven unbekannter Formate) entdeckt werden

Systemanforderungen

- HDD: 50 MB
- Betriebssystem: Microsoft Windows 2000/XP/Vista, Microsoft Windows Server 2000/2003/2008 (32- und 64-Bit-Versionen)
- Proxy-Server: Qbik WinGate 6

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/gateway/qbik/

© Doctor Web, 2016

Dr.Web für Microsoft ISA Server und Forefront TMG

Viren- und Spamprüfung von Daten, die per Microsoft ISA Server und Forefront TMG übertragen werden

Vorteile

- Viren- und Spamprüfung von Dateien in kürzester Zeit durch Technologien der dynamischen Analyse der Systemauslastung und die Umschaltung zwischen verschiedenen Aufgaben
- Einsatz neuester Plattformen für einen höheren Scan-Durchsatz
- Arbeit auf Servern beliebiger Konfiguration, u.a. mit einem geringen Hauptspeicher
- Schutz für reale und virtuelle Server
- Integrierte Antispam-Komponente, die kein Training erfordert und sofort nach der Installation zu funktionieren beginnt. Das Antispam-Modul sorgt für eine geringere Serverauslastung und fördert die Arbeitsfähigkeit der Mitarbeiter.
- Sperrung des Zugriffs auf bestimmte Web-Inhalte, die als Malwarequellen dienen
- Einzigartige Technologien für die Entdeckung neuester Packprogramme
- Installation und Konfiguration je nach Unternehmensbedarf

Schlüsselfunktionen

- Viren- und Spamprüfung sämtlicher Daten, die übertragen werden
- Prüfung von eingehenden Dateien „on the fly“ und Entdeckung von Malware in gepackten Dateien
- Desinfektion infizierter Dateien
- Durchführung verschiedener Aktionen je nach Spamtyp
- Begleitende Nachricht für E-Mails, die Sicherheitsbedrohungen enthalten
- Sperrung des Zugriffs auf infizierte Dateien für alle Benutzer eines lokalen Netzwerks
- Einschränkung des Zugriffs der Benutzer auf bestimmte Web-Inhalte durch Office Control
- Verschiebung verdächtiger und infizierter Dateien in die Quarantäne
- Benachrichtigung des Administrators über Virenfunde
- Protokollieren der Funktion des Programms
- Automatisches Update

System- und Programmanforderungen

Für Microsoft ISA Server:

- Pentium III 733 MHz und höher
- Hauptspeicher: 1 GB und größer
- HDD: 300 MB für die Installation. Zusätzlicher Freiplatz für temporäre Dateien während der Virenprüfung.
- Betriebssystem: Microsoft Windows Server 2003 x86 Service Pack 1 (SP1), Microsoft Windows Server 2003 R2 x86
- Proxy-Server: Microsoft ISA Server 2004, Microsoft ISA Server 2006

Für Microsoft Forefront TMG:

- Pentium III 1.86 GHz und höher
- Hauptspeicher: 2 GB und größer
- HDD: 300 MB für die Installation. Zusätzlicher Freiplatz für temporäre Dateien während der Virenprüfung.
- Betriebssystem: Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2008 R2
- Proxy-Server: Microsoft ForefrontTMG 2010

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/gateway/isa/

© Doctor Web, 2016

Dr.Web Mobile Security Suite

Schutz für mobile Endgeräte

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

	Dr.Web für Symbian OS	Dr.Web für Windows Mobile	Dr.Web für Android
Schutzkomponenten	Antivirus + Antispam	Antivirus + Antispam	Antivirus + Antispam
Zentrale Verwaltung in Dr.Web Enterprise Security Suite	–	+	–
Unterstützte Betriebssysteme	S60, Symbian 9 und höher	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5	Android OS: 4.0-5.0
Schlüsselfunktionen			
Prüfung «on the fly»	+	+	+
Prüfung von Dateien, die per GPRS/Infrarot/ Bluetooth/Wi-Fi/ USB während der Synchronisierung übertragen werden	+	+	+
Zwei Prüfungsmodi: vollständig und benutzerdefiniert	+	+	+
Option der Aktivierung/ Deaktivierug der permanenten Prüfung der Speicherkarte	–	+	+
On-Demand-Prüfung des ganzen Dateisystems oder einzelner Dateien bzw. Verzeichnisse	+	+	+
Prüfung von Dateien in ZIP-, SIS-, CAB- und RAR-Archiven	+	+	+
Black- und Whitelists für eingehende Anrufe und SMS	+	+	+
Löschen infizierter Dateien	+	+	+

© Doctor Web, 2016

Verschiebung verdächtiger Dateien in die Quarantäne	+	+	+
Wiederherstellen von Dateien aus der Quarantäne	+	+	+
Update via Internet: ■ Per HTTP durch das GPRS-Modul ■ Per Infrarot/ Bluetooth/Wi-Fi/USB ■ Durch die Synchronisierung des PCs mir einer Internetverbindung via ActiveSync	+	+	+
Detailliertes Protokoll über die Prüfung des Systems	+	+	+

Lizenzierung für Dr.Web Mobile Security Suite

Dr.Web für mobile Engeräte wird je nach Anzahl der zu schützenden mobilen Endgeräte lizenziert.

Lizenzvarianten

Dr.Web für Windows Mobile	Dr.Web für Symbian OS	Dr.Web für Android
■ Antivirus + Antispam + Verwaltungscenter	■ Antivirus + Antispam	■ Rundumschutz + Verwaltungscenter

Dr.Web für mobile Engeräte ist auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

Sonderangebot

Eine Gratis-Lizenz für Dr.Web Mobile Security Suite bekommen alle registrierten Anwender von:

- Dr.Web Box-Produkten
- Dr.Web Security Space
- Dr.Web Antivirus für Windows/OS X/Linux

Nützliche Links

Produktbeschreibung: http://products.drweb-av.de/mobile/

© Doctor Web, 2016

Dr.Web Retail Security Suite: Produkte für Retail

Dr.Web Security Space

2 PCs/1 Jahr

Dr.Web Antivirus

2 PCs/1 Jahr

Dr.Web Security Space + Dr.Web Antivirus für OS X

2 PCs/2 Jahre

Small Business Bundle

5 PCs/1 Server/5 E-Mail-Adressen/1 Jahr

© Doctor Web, 2016

Dr.Web Bundles

Dr.Web Bundles enthalten Dr.Web Produkte für alle Typen von Objekten.

WICHTIG! Für das Bundle werden keine Preisnachlässe (u.a. für die Lizenzverlängerung) angewendet. Um das Bundle weiter benutzen zu können, müssen Sie eine neue Lizenz zum Vollpreis erwerben. Der Preisvorteil für die Lizenzverlängerung wird beim Umsteig vom Bundle auf einzelne Dr.Web Produkte gewährt.

Dr.Web Universal Bundle

Kostengünstiger Rundumschutz der Enterprise-Klasse für kleine und mittelständische Unternehmen

Kleine Untenehmen verfügen häufig über keine großen Budgets für den Rundumschutz. Für diese Unternehmen (mit 5-50 PCs) ist Dr.Web Universal Bundle gedacht.

Dr.Web Universal Bundle + Kryptograph wird zusammen mit Lizenzen für Atlansys Bastion Pro geliefert*.

Produkt	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
Geschützte Objekte	Workstations	Server	E-Mail-Anwender	Anwender von E-Mail- und Internet-Gateways	Mobile Endgeräte
Lizenz	Rundumschutz	Antivirus	Antivirus + Antispam	Antivirus	Antivirus + Antispam
Umfang	5 - 50	1	Entspricht der Anzahl von Workstations	Entspricht der Anzahl von Workstations (ab 25)	Entspricht der Anzahl von Workstations

* Atlansys Bastion Pro ist ein Produkt von Atlansys (www.atlansys.ru)

Nützliche Links

Dr.Web Bundles: http://products.drweb-av.de/bundles/universal/

Dr.Web School Bundle

Geschützte Objekte	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Lizenz	Rundumschutz + Verwaltungscenter	Antivirus	
Umfang	10 – 200	1 – 8	10 – 200

Nützliche Links

Dr.Web Bundles: http://products.drweb-av.de/bundles/safe_school/

© Doctor Web, 2016

Tools

Dr.Web Desinfektions-Tools sind für die Diagnose und Not-Desinfektion gedacht. Sie bieten keinen permanenten Schutz für Ihren Computer.

Dr.Web CureNet!

Zentral verwaltete Desinfektion lokaler Netzwerke jeder Größenordnung (u.a. bei der installierten Antivirensoftware eines anderen Herstellers)

Potenzielle Anwender	Kleine, mittelständische und große Unternehmen, in deren lokalen Netzwerken Antivirenprogramme anderer Hersteller installiert sind
Aufgaben	■ Zentrale Prüfung und Desinfektion von Workstations und Servern, wenn die Antivirensoftware eines anderen Herstellers versagt ■ Qualitätstest für das Antivirenprogramm eines anderen Herstellers
Besonderheiten des Tools	■ Deinstallation des Antivirenprogramms eines anderen Herstellers vor der Prüfung und Desinfektion ist nicht erforderlich ■ Installation des Servers oder anderer Software ist nicht erforderlich ■ Möglichkeit der Verwendung in Netzwerken ohne Internetverbindung ■ Der Dr.Web CureNet! Assistent kann von einem beliebigen externen Datenträger (u.a. vom USB-Speicher) gestartet werden
Produktbeschreibung	http://curenet.drweb.com/
Unterstützte Betriebssysteme	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32 und 64 Bit)
Was ist "Mein Dr.Web CureNet!"?	Dies ist Ihr persönlicher Bereich, wo Sie während der ganzen Lizenzlaufzeit Ihren persönlichen Link zum aktuellen Download finden. Aus dem persönlichen Bereich können Sie den technischen Support kontaktieren, eine verdächtige Datei zur Analyse einreichen sowie weitere Services nutzen.
Lizenzierung	Das Tool wird nach Anzahl zu schützenden Workstations (mind. 5) für 1, 2 und 3 Jahre lizenziert.
Demoversion	Ohne Funktion der Desinfektion
Systemanforderungen	Assistent ■ Beliebiger PC unter MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32 und 64 Bit) ■ Hauptspeicher: mind. 360 MB ■ HDD: mind. 200 MB ■ Verbindung zu allen geschützten Workstations via TCP/IP ■ Internetverbindung: zum Update von Virendatenbanken und Komponenten von Dr.Web CureNet! Scanner ■ Beliebiger PC unter MS Windows XP Professional und höher außer Windows® Server 2003 x64 Edition und Windows® XP Professional SP2 x64 Edition ■ Hauptspeicher: mind. 360 MB ■ HDD: mind. 200 MB

© Doctor Web, 2016

Dr.Web CureIt!

Not-Desinfektion von PCs und Servern unter Windows (u.a. bei der installierten Antivirensoftware eines anderen Herstellers)

Potenzielle Anwender	Kleine, mittelständische und große Unternehmen, in deren lokalen Netzwerken Antivirenprogramme anderer Hersteller installiert sind
Aufgaben	■ Zentrale Prüfung und Desinfektion von Workstations und Servern, wenn die Antivirensoftware eines anderen Herstellers versagt ■ Qualitätstest für das Antivirenprogramm eines anderen Herstellers
Beonderheiten des Tools	■ Dr.Web CureIt! erfordert keine Installation und ist mit beliebigen Antivirenprogrammen kompatibel. Das installierte Antivirenprogramm eines anderen Herstellers muss dabei nicht ausgeschaltet werden ■ Dr.Web CureIt! verfügt über einen hervorragenden Selbstschutz und kann Windows-Blockern einen effizienten Widerstand leisten ■ Dr.Web CureIt! wird mehrmals pro Stunde aktualisiert ■ Das Tool kann von einem beliebigen externen Datenträger aus (u.a. USB-Speicher) gestartet werden
Produktbeschreibung	http://free.drweb.com/cureit/
Unterstützte Betriebssysteme	MS Windows XP/2003/Vista/2008/7/8/2012/10 (32 und 64 Bit)
Lizenzierung	Das Tool wird für 12, 24 und 36 Monate lizenziert.
Besonderheiten der Lizenzierung	Das Tool ist kostenlos für die Desinfektion Ihres eigenen Home-PCs
Demoversion	Nein

© Doctor Web, 2016

Lösungen

Dr.Web Security Suite für UNIX Appliance ist eine modulare Gruppe von Lösungen, die für die Integration mit den auf UNIX (Linux/FreeBSD/Solaris(x86)) basierenden Appliances gedacht sind.

Die Lösungen haben die Funktion des Internet-Gateways des Unternehmens (Proxy-Server, der für die Einrichtung des Zugriffs auf Internet-Inhalte für Intranet-Anwender verwendet wird).

	Dr.Web Mail Security Suite für UNIX Appliance	**Dr.Web Gateway Security Suite für UNIX Appliance**
Schlüsselfunktion	Filterung von E-Mails auf Viren und Spam	Filterung von HTTP- und FTP-Daten auf Viren
Lizenzvarianten	Antivirus Antivirus + Antispam	Antivirus

Lizenzierung

- Nach Anzahl der zu schützenden Anwender (unbeschränkt)
- Lizenz pro Server (zur Prüfung des unbeschränkten E-Mail-Verkehrs auf einem Server mit bis zu 3 000 zu schützenden Anwendern)

Lizenzierung für SDK

SDK wird inklusive mit dem Produkt verbreitet. Unabhängige Entwickler können Plug-ins anhand SDK unter nicht kommerziellen Bedingungen uneingeschränkt entwickeln und verbreiten. Die kommerzielle Nutzung von SDK bedarf der Zertifizierung.

© Doctor Web, 2016

Services

Software as a service (kurz SaaS) ist ein beliebtes Software-Distributions-Modell mit der Philosophie, Software als Dienstleistung bereitzustellen.

Im Mai 2007 führte der russische Sicherheitsspezialist den Managed Security Service Dr.Web AV-Desk ein. So entstand ein neues Segment am russischen IT-Sicherheitsmarkt. Dr.Web Antivirus wurde im SaaS-Modell angeboten.

Managed Security Service Dr.Web AV-Desk

Was ist Dr.Web AV-Desk?	Dr.Web AV-Desk ist ein **Managed Security Service** für IT-Anbieter, die einer unbeschränkten Anzahl an Privat- und Business-Kunden Dienstleistungen in Sachen IT-Sicherheit online anbieten können. Dr.Web AV-Desk ist eine **Software**, durch die der Abo-Service für Dr.Web Antivirus verwaltet werden kann. Dr.Web AV-Desk ist ein **VAD-Geschäftsmodell**, mit dem IT-Anbieter Neukunden gewinnen und ihre Einnahmen steigern können.
Für welche Anbieter ist Dr.Web AV-Desk gedacht?	Internetanbieter und Unternehmen, die im IT-Bereich aktiv sind
Für wen ist Dr.Web Antivirus gedacht?	Privat- und Business-Kunden (Kunden von IT-Anbietern)
Welche Services kann der Service-Anbieter mit Dr.Web AV-Desk anbieten?	IT-Sicherheitsservices für Kunden der IT-Anbieter gegen Viren, Spam und sonstige Malware. IT-Sicherheitsservices sind als Abos mit einer gewünschten Laufzeit verfügbar. Für die Nutzung von Funktionen der **Dr.Web Software** ist eine Abo-Gebühr fällig.
Funktionalität von Dr.Web AV-Desk	Software für eine zentrale Verwaltung der IT-Sicherheitsservices für Kunden der IT-Anbieter
Lizenzierung für Dr.Web AV-Desk	Die Serversoftware von Dr.Web AV-Desk wird dem Anbieter kostenlos zur Verfügung gestellt. Die Agenten-Software von Dr.Web AV-Desk wird nach der Anzahl der Kunden mit einem gültigen Abo in einer Bilanzperiode (Monat) lizenziert.

© Doctor Web, 2016

Wie funktioniert es?

Lieferant	Kunde
■ bietet die Möglichkeit, Dr.Web Antivirus im SaaS-Modell über das Abo-Verwaltungscenter zu abonnieren ■ bietet Updates der Dr.Web Virendatenbanken und Programm-Module an ■ bietet den technischen Support an (optional) ■ überwacht die Sicherheitslage im Antivirus-Netzwerk und sammelt statistische Daten über Vireninfektionen ■ bietet zusätzliche Services an ■ erhebt eine Abo-Gebühr	■ erstellt ein Abo im Abo-Verwaltungscenter ■ installiert die Dr.Web Software ■ konfiguriert die Abo-Parameter ■ zahlt eine Abo-Gebühr an den Service-Anbieter

Dr.Web AV-Desk ist ein vielseitiges Geschäftsmodell. Als Lieferanten des Dr.Web Antivirus-Services können Internetanbieter sowie andere Unternehmen, die im IT-Bereich tätig sind, auftreten.

	Reseller des Dr.Web Antivirus-Services	Anbieter des Dr.Web Antivirus-Services	Service-Aggregator für Dr.Web AV-Desk
Geschäftsfeld	Das Unternehmen bietet Endanwendern Dr.Web Antivirus-Service über das Abo-Verwaltungscenter auf seiner Website an.	Das Unternehmen führt Dr.Web AV-Desk ein und bietet Endanwendern Dr.Web Antivirus im SaaS-Modell an.	Das Unternehmen verfügt über Server, auf denen Dr.Web AV-Desk eingerichtet wird, baut ein Reseller-Netzwerk auf und sublizenziert für Reseller Abo-Verwaltungscenter. Dabei sind die Reseller nicht berechtigt, den Antivirus-Service Endkunden anzubieten.

Detaillierte Informationen über Dr.Web AV-Desk und Dr.Web Antivirus-Service werden Partnern auf Anfrage zur Verfügung gestellt.

© Doctor Web, 2016

Rabattpolitik

Der Rabattquotient wird anhand der aktuellen Preisliste für den Preis einer 1-Jahres-Lizenz angewendet. Wenn der Benutzer Anspruch auf mehrere Rabatte hat, werden sie nicht kumuliert, sondern der Benutzer bekommt den höchsten Rabatt (exkl. Rabatte für Internetanbieter).

Die Rabatte gelten nur für die in der Preisliste stehenden Lösungen. Die Rabatte für andere Produkte und Lösungen bedürfen der Einwilligung eines Doctor Web Managers.

Rabatte für die Menge der lizenzierten Produkte von Dr.Web Enterprise Security Suite

Die Rabatte für die Menge der lizenzierten Produkte hängen vom Preis für Basislizenzen und zusätzliche Komponenten für jedes einzelne Produkt ab. Diese Rabatte werden automatisch berücksichtigt.

Menge der lizenzierten Produkte	Rabatt
4	30%
3	25%
2	20%

Ausnahme: Es gelten keine Rabatte für Dr.Web Mobile Security Suite

Einschränkungen

Die Rabatte werden nicht angewendet, wenn:

- die Menge der Server unter 10% der Anzahl von Workstations, E-Mail-Anwender und Gateways liegt
- die Anzahl der E-Mail-Anwender oder Gateways weniger ist als die Anzahl der Workstations
- die Anzahl der Gateway-Anwender weniger ist als die Anzahl der E-Mail-Anwender und umgekehrt

Rabatte im Vergleich

Kunde	Grund	Neue Lizenz			Verlängerung			Migration		
		1 Jahr	2 Jahre	3 Jahre	1 Jahr	2 Jahre	3 Jahre	1 Jahr	2 Jahre	3 Jahre
Regulär	Für Verlängerungsrabatte: Schlüsseldatei oder Seriennummer mit mind. 3 Monaten Laufzeit für ein vergleichbares Dr.Web Produkt	–	1,6	2,17	0,6	1,17	1,72	0,5	1	1,5
	Für Migrationsrabatte: Lizenzoriginal/Schlüsseldatei/Bestätigung für den Kauf einer elektronischen Version von Antivirensoftware eines anderen Herstellers									
Lehre und Schule, Bibliotheken und Medizineinrichtungen	Kopie eines Registerauszuges und ausgefüllter Fragebogen	0,5	0,85	1,2	0,35	0,7	1,05			

© Doctor Web, 2016

Verlängerungsbedingungen

1. Es kann sowohl eine gültige als auch eine ungültige (bereits abgelaufene) Lizenz mit einem Preisvorteil verlängert werden. Die Gültigkeit der Lizenzverlängerung kann nicht verjähren.
2. Der Preisvorteil wird auch bei der Verlängerung der Lizenz für das vergleichbare Dr.Web Produkt oder die vergleichbare Dr.Web Lösung gewährt. Die Laufzeit einer solchen Lizenz sollte mindestens 6 Monate sein.
3. Der Verlängerungsrabatt wird beim Kauf einer 1-, 2- oder 3-Jahres-Lizenz für das vergleichbare Dr.Web Produkt oder die vergleichbare Dr.Web Lösung gewährt.
4. Die Lizenzverlängerung mit einem Preisvorteil gilt für die gleiche Anzahl geschützter Objekte wie in der vorherigen Lizenz.
5. Der Grund für die Gewährung eines Verlängerungsrabatts ist eine Schlüsseldatei oder eine Seriennummer. Dabei kann die entsprechende Lizenz nur einmal verlängert werden.
6. Um einen Preisvorteil zu bekommen, soll der Anwender dem Händler eine Seriennummer oder Schlüsseldatei (u.a. OEM-Schlüsseldatei) vorlegen.

Preisvorteile

„Umsteigen auf Grün!" ist ein Migrationsprogramm für Anwender der Antivirensoftware anderer Hersteller

1. Das vorliegende Sonderangebot gilt für alle Dr.Web Produkte. Bundles, Tools, Appliances, Services und Lösungen sind vom Migrationsprogramm ausgenommen.
2. Die Preisvorteile richten sich nicht an Privatpersonen, sondern an Einrichtungen und Unternehmen, die sie nur einmal beanspruchen können.
3. OEM-Lizenzen sind vom Migrationsprogramm ausgenommen.
4. 50% Preisnachlass wird Benutzern einer anderen Antivirensoftware gewährt, welche von ihrer ursprünglichen Lizenz auf Dr.Web umsteigen. Bei der Migration auf eine 2- bzw. 3-Jahres-Lizenz wird der Preis für eine 1-Jahres-Lizenz jeweils mit dem Faktor 1 und 1,5 multipliziert.
5. Ein Preisvorteil bei der Migration gilt für eine vergleichbare Dr.Web Lösung (nach Typ und Anzahl der geschützten Objekte).
6. Um bei der Migration einen Preisvorteil zu erhalten, muss der Anwender eine Schlüsseldatei bzw. eine Kaufbestätigung mit Registrierungsdaten für die elektronische Lizenz eines anderen Herstellers vorlegen.
7. Der Preisnachlass wird Anwendern sowohl gültiger als auch abgelaufener Lizenzen gewährt, wenn der Anwender einen Fachhändler von Doctor Web innerhalb von 30 Tagen nach Lizenzablauf kontaktiert hat.
8. Wenn die Laufzeit der Antivirensoftware eines anderen Herstellers zum Zeitpunkt der Bezahlung einer Migrationslizenz nicht abgelaufen ist, wird die Restlaufzeit Ihrer vorherigen Lizenz mit der Laufzeit Ihrer neuen Lizenz zusammen addiert.
9. Bei der nächsten Verlängerung der Migrationslizenz wird ein regulärer Preisvorteil gewährt.
10. Preisvorteile im Rahmen dieses Migrationsprogramms werden mit keinen anderen Preisvorteilen zusammen addiert.

Nützliche Links

http://promotions.drweb-av.de/promo/migrate/

© Doctor Web, 2016

Allgemeine Verkaufsbedingungen

1. Die Partner verpflichten sich, Dr.Web Antivirensoftware an Endanwender im festgelegten Umfang und laut empfohlener Preisliste zu verkaufen.
2. Für alle Dr.Web Produkte im Standardumfang sind Updates der Programm-Module und Virendatenbanken sowie der technische Support über das Web-Formular unter http://support.drweb-av.de während der ganzen Lizenzlaufzeit im Lizenzpreis enthalten.
3. Bei der Bestellung von Lizenzen in einer Firmen-Box wird der Lizenzpreis um den Preis eines Mediapakets erhöht.
4. Wenn der Käufer eine Virenschutz-Lösung für mehr Objekte braucht, als in der Preisliste angegeben, soll der Partner entsprechende Preise bei Doctor Web anfordern und über das Web-Formular https://pa.drweb.com/support/ folgende Kundendaten übermitteln:
   - Firmenname
   - Anschrift
   - E-Mail-Adresse
   - Telefon des zuständigen Mitarbeiters
   - Kontaktdaten des technischen Supports des Partners
   - Alle Rabatte werden dem Endanwender nur beim Kauf entsprechender Lösungen gewährt und bedürfen der Abstimmung mit Doctor Web
5. Preise für Lösungen, die in der vorliegenden Preisliste nicht enthalten sind, werden durch die Lizenzvereinbarung bestimmt, die zwischen Doctor Web und dem Lieferanten solcher Lösungen für Endanwender getroffen wird.

Lizenzerweiterung für Dr.Web Enterprise Security Suite

Allgemeine Regeln

1. Die Lizenzerweiterung während der Lizenzlaufzeit kann wie folgt sein:
   - **Qualitativ**
     Die laufende Lizenz wird um neue Komponenten erweitert. Der Produktumfang bleibt unverändert.
   - **Quantitativ**
     Die Anzahl der zu schützenden Objekte für die laufende Lizenz wird erhöht.
   - **Produkterweiterung**
     Für die laufende Lizenz kommen neue Produkte hinzu.

Die Lizenzerweiterung kann auch kombiniert sein:

2. Minimale Lizenzlaufzeit bei der Lizenzerweiterung: 3 Monate / Maximale Lizenzlaufzeit: 33 Monate.
3. Die Restlaufzeit wird in Monaten berechnet; dabei wird der laufende Monat aufgerundet.
4. Lizenzerweiterungen ohne Verlängerung sind nur für bestehende Lizenzen mit mindestens 3 Monaten Restlaufzeit möglich. Ansonsten ist zur Lizenzerweiterung eine Lizenzverlängerung notwendig.
5. Typ der neuen Lizenz: C (Lizenzerweiterung).
6. Die erweiterte Lizenz wird automatisch während ihrer Generierung aktiviert.
7. Die vorherige Lizenz wird 24 Stunden nach der Aktivierung der neuen Lizenz deaktiviert. Die alte Lizenz kann nicht mehr verlängert werden. Für die Verlängerung müssen Sie Ihre erweiterte Lizenz vorweisen.

© Doctor Web, 2016

Lizenzerweiterung mit Verlängerung

1. Die Lizenzerweiterung mit der Lizenzverlängerung ist sowohl für gültige Lizenzen als auch abgelaufene Lizenzen möglich.
2. Bei der Erweiterung einer gültigen Lizenz wird die Restlaufzeit mit der Laufzeit Ihrer neuen Lizenz (Erweiterung mit Verlängerung) addiert.
3. Lizenztyp im Coder der neuen Lizenz: D (Erweiterung+Verlängerung).
4. Die erweiterte Lizenz wird automatisch während ihrer Generierung aktiviert.
5. Die vorherige Lizenz wird 24 Stunden nach der Aktivierung der neuen Lizenz deaktiviert. Die alte Lizenz kann nicht mehr verlängert werden. Für die Verlängerung müssen Sie Ihre erweiterte Lizenz vorweisen.
6. Bei gleichzeitiger Verlängerung und Erweiterung Ihrer Lizenz wird der Preis für zugekaufte Lizenzen anhand der folgenden Regeln kalkuliert.

Preiskalkulation für neue Lizenzen

I. Qualitative Lizenzerweiterung (Die Lizenz wird um zusätzliche Komponenten erweitert. Die Anzahl der zu schützenden Objekte und der Produktumfang bleiben unverändert.):

1. Wenn eine **Erweiterung von Antivirus auf Rundumschutz für Dr.Web Desktop Security Suite** vorgenommen wird, wird für die restlichen Monate ein Aufpreis in Höhe von 20% des Preises einer Lizenz für Antivirus, geteilt durch die restlichen Monate bis zum Ablauf Ihrer Lizenz erhoben.

Beispiel:

Die neue Antivirus-Lizenz für 90 Rechner kostet €1.223, zwei Monate nach dem Kauf möchte der Kunde auf Rundumschutz erweitern. Daraus ergäben sich

€1.223 × 20*Proz* × ((12 − 2)*Monate* ÷ 12*Monate*) = €1.223 × 0,20 × (10 ÷ 12) = €203,83 *Aufpreis*

Neuer Endpreis der Lizenz: **€1.426,83**

2. Wenn die **Antispam**-Komponente für Dr.Web Mail Security Suite oder Dr.Web Gateway Security Suite erforderlich ist, wird ein Aufpreis in Höhe von 40% vom Preis einer Lizenz für Dr.Web Antivirus oder Dr.Web Antivirus + SMTP-Proxy angewendet.

Beispiel:

Die ursprüngliche Jahreslizenz für 90 Benutzer kostet €976, nach zwei Monaten möchte der Kunde auf Antispam erweitern. Daraus ergäben sich

€976 × 40*Proz* × ((12 − 2)*Monate* ÷ 12*Monate*) = €976 × 0,40 × (10 ÷ 12) = €325,33*Aufpreis*

Neuer Endpreis der Lizenz: **€1.301,33**

3. Wenn eine Lizenz für Dr.Web Mail Security Suite um die Komponente **SMTP-Proxy** ergänzt wird, wird für die restlichen Monate ein Aufpreis in Höhe von 20% des Preises einer Lizenz für Antivirus bzw. Antivirus mit Antispam erhoben.

© Doctor Web, 2016

Aufpreise bei qualitativer Lizenzerweiterung ohne Erhöhung der Anzahl der zu schützenden Objekte

Produkt	Laufende Lizenz	Neue Lizenz	Aufpreis
Dr.Web Desktop Security Suite	Antivirus	Rundumschutz	20%
Dr.Web Mail Security Suite oder Dr.Web Gateway Security Suite	Antivirus	+ Antispam	40%
	Antivirus + SMTP-Proxy		
	Antivirus	+ SMTP-Proxy	20%
	Antivirus + Antispam		

II. Quantitative Lizenzerweiterung (Anzahl der zu schützenden Objekte wird erhöht)

Der Preis für zugekaufte Lizenzen wird anhand der gültigen Preisliste **ohne Rabatte** kalkuliert.

III. Produkterweiterung (Erweiterung des Produktumfanges)

Der Preis für zugekaufte Lizenzen wird anhand der gültigen Preisliste **ohne Rabatte** kalkuliert.

Produkte für Geschäftskunden, für die eine Lizenzerweiterung nicht möglich ist:

- Box-Produkt Dr.Web Small Business Bundle
- Dr.Web Universal Bundle
- Dr.Web School Bundle

Um eine Lizenz dieser Produkte zu erweitern, müssen Sie auf das Produkt Dr.Web Enterprise Security Suite zum Preis einer Lizenzerweiterung mit Lizenzverlängerung umsteigen.

© Doctor Web, 2016

Lizenzcodes für Dr.Web Produkte, Bundles, Tools und Appliances

Regeln für die Erstellung von Lizenzcodes

1. Der Code besteht immer aus 5 Gruppen.
2. Jede Gruppe ist von der anderen durch einen Bindestrich getrennt. Der Code der Lizenz für „Produkte“ wird für jedes kommerzielle Dr.Web Produkt separat erstellt (siehe „Produktpalette Dr.Web Security Suite“).
3. Die Codes für Appliances Dr.Web Office Shield bestehen aus 2 Codes:
   - Hardwarecode
   - Lizenzcode
4. Die Codes für Box-Produkte, Scratch-Karten und Mediapakete sowie für Hardware von Dr.Web Office Shield finden Sie in der Preisliste (fix).
5. Im Code der Lizenz „Zukauf“ werden 2 Laufzeiten angegeben: Gesamtlaufzeit der zuzukaufenden Lizenz und – durch Semikolon getrennt – die Restlaufzeit des gültigen Schlüssels.
6. Im Code der Lizenz „Zukauf + Verlängerung“ werden 2 Laufzeiten angegeben: Gesamtlaufzeit von Lizenzen, die zugekauft und verlängert werden sollen, und – durch Semikolon getrennt – die Restlaufzeit des zu verlängernden Schlüssels.
7. Im Code der Lizenz „Zukauf“ werden 2 Gruppen der zu schützenden Objekte angegeben: Gesamtzahl von Lizenzen (u.a. für den Zukauf) und – durch Semikolon getrennt – Anzahl von Objekten für Ihre gültige Lizenz.
8. Im Code der Lizenz „Zukauf + Verlängerung“ werden 2 Gruppen der zu schützenden Objekte angegeben: Gesamtzahl von Lizenzen (u.a. für den Zukauf und die Verlängerung) und – durch Semikolon getrennt – Anzahl von Objekten für Ihre gültige Lizenz.

© Doctor Web, 2016

Symbole und Codes

Gruppe 1			Gruppe 2		Gruppe 3	Gruppe 4	Gruppe 5	
Umfang	**Produktkategorie**	**Geschützte Objekte**	**Basislizenz**	**Zusätzliche Komponenten**	**Lizenzlaufzeit**	**Anzahl geschützter Objekte**	**Lizenztyp**	**Preisvorteil**
L – Produkt, das von der Website heruntergeladen wird	**B** – Produkt für Business **H** – Produkt für Privat	**G** – Gateway-Anwender	**A** – Antivirus	**A** – Antispam	**XXM,** – wo XX die Anzahl von Monaten ist	Beliebige Zahl	**A** – Neue Lizenz	**1** – Bildungs-, Medizineinrichtung, Bibliotheken und Museen
B – Produkt in der Karton-Box	**X** – Produkt, das zusammen mit Dr.Web Office Shield geliefert wird	**M** – Mobile Endgeräte	**B** – Rundumschutz	**C** – Verwaltungscenter	**XXXD,** – wo XXX die Tagesanzahl ist	**UL** – Unbegrenzt (für eine unbegrenzte Lizenz)	**B** – Lizenzverlängerung **C** – Lizenzerweiterung	**2** – Aktion **3** – Kein Preisvorteil
A – Produkt in der Aktions-Box	**Y** – Tool	**P** – E-Mail-Anwender	***** – Lizenzen für mehrere Produkte (gültig nur für Bundles)	**K** – Keine zusätzlichen Komponenten			**D** – Lizenzverlängerung mit der Lizenzerweiterung	**4** – Migration
C – Karte mit einem Rubbelstreifen	**Z** – Bundle	**S** – Server					**F** – OEM-Lizenz	**5** – NFR-Lizenz für Partner
D – Produkt in der DVD-Packung		**W** – Workstations		**S** – SMTP-Proxy			**G** – Service-Lizenz	**6** – NFR-Lizenz (Demo) für Kunden
K – Produkt im Lizenzpaket		**Z** – Alle Objekte						**7** – Marketing-/Ausbildungsbedarf
M – Produkt auf der Firmen-CD (inkl. OEM)								**8** – Wohltätigkeit
N – Produkt im zertifizierten Mediapaket								**9** – Aufteilung eines Schlüssels
P – Produkt im Mediapaket für OEM-Lizenzen								**10** – Vereinigung mehrerer Schlüssel
								11 – Schlüsselwechsel

© Doctor Web, 2016

Kontakt

Russische Föderation

Doctor Web Ltd.

Tretja uliza Jamskogo polja 2-12A, 125124, Moskau
Tel.: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
Internet: www.drweb.com | www.av-desk.com | www.freedrweb.com

China

Doctor Web Software Company (Tianjin), Ltd.

112, North software tower, №80, 4th Avenue, TEDA, Tianjin, China
天津市经济技术开发区第四大街80号软件大厦北楼112
Tel: +86-022-59823480
Fax: +86-022-59823480
E-mail: y.zhang@drweb.com
Internet: www.drweb.cn

Deutschland

Doctor Web Deutschland GmbH

Platz der Einheit 1
60327 Frankfurt
Tel.: + 49 (0)69 975 03 137
Fax: + 49 (0)69 975 03 200
Internet: www.drweb-av.de

Frankreich

Doctor Web France

333b, Avenue de Colmar, 67100 Strasbourg
Tel.: 04 90 40 20 20
Fax.: 04 90 40 20 21
E-Mail: p.curien@drweb.com
Internet: www.drweb.fr

Japan

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F,
1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi,Kanagawa-ken
210-0005, Japan
Tel: +81(0)44-201-7711
Internet: www.drweb.co.jp

Republik Kazachstan

Doctor Web Zentralasien

Shevchenko 165B, Büro 910, 05009 Almaty
Tel.: +7 (727) 323-62-30, 323-62-31, 323-62-32
Vertrieb: sales@drweb.kz
Technischer Support: http://www.drweb.kz/support, support@drweb.kz
Internet: www.drweb.kz

Ukraine

Doctor Web Ukraine

01601, Ukraine, Kiev, Pushkinskaya, 27, office 6
Tel./Fax: +38 (044) 238-24-35
E-Mail: info@drweb.ua
Internet: www.drweb.ua

© Doctor Web, 2016