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.
Das Unternehmen verfügt über eine 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.
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.

Russische Föderation	**Doctor Web** Tretja uliza Jamskogo polja 2, Geb.12A, 125124 Moskau, Russische Föderation Tel.: +7 (495) 789-45-87 Fax: +7 (495) 789-45-97 www.drweb.com | www.av-desk.com | www.freedrweb.com
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 www.drweb-av.de
Frankreich	**Doctor Web France** 333 b Avenue de Colmar, 67100 Straßburg, Frankreich Telefon: + 33 (0) 3-90-40-40-20 Fax : + 33 (0) 3-90-40-40-21 www.drweb.fr
Republik Kazachstan	**Doctor Web – Zentralasien** Shevchenko 165B, Büro 910, 05009 Almaty, Republik Kazachstan Tel.: +7 (727) 323-62-30, 323-62-31, 323-62-32 www.drweb.kz
Ukraine	**Doctor Web Technischer Support** Uliza Kostelnaja 4-3, 01001 Kiev, Ukraine Telefon/Fax: +380 (44) 238-24-35, +380 (44) 279-77-70 www.drweb.com.ua
Japan	**Doctor Web Pacific, Inc.** NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005, Japan Telefon: +81 (0) 44-201-7711 www.drweb.co.jp
China	**Doctor Web Software Company (Tianjin), Ltd.** Add: 112, North software tower, 80, 4th Avenue, TEDA, Tianjin, China E-mail: d.liu@drweb.com

Funktionalität

Desinfektion von PC und Servern	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)
Desinfektion für Netzwerke, die keine Internetverbindung haben	Einschließlich IPv6
Netzwerkgröße	Unbeschränkt
Installation des **Dr.Web CureNet!** Assistenten	Beliebiger PC unter MS Windows XP Professional und höher außer Windows® Server 2003 x64 Edition und Windows® XP Professional SP2 x64 Edition
Verbreitung der Desinfektions-Scanner über USB-Datenträger	■
Installation der Dr.Web Scanner für Windows	Nicht erforderlich
Scanner werden auf allen/benutzerdefinierten Hosts per Fernzugriff zentral gestartet	■
Benutzerdefinierte Virenprüfung auf Fern-Workstations	■
Unterbrechen oder Abbrechen der Virenprüfung auf ausgewählten Workstations	■
Ausschalten des Netzwerkzuganges für benutzerdefinierte Workstations, um die wiederholte Infizierung zu vermeiden	■
Zentrale Einstellung von Aktionen für detektierte Malware-Objekte	■
Zentrale Erhebung der Statistiken	■
Automatische Entfernung der Scanner nach der durchgeführten Prüfung	■
Export des Scan-Protokolls	■
Workstation-Suche	
Automatische Suche nach ■ IP-Adresse ■ IP-Adressenbereich ■ Maske ■ Netzwerknamen	■
Prüfung	
Benutzerdefinierte Scan-Profile	■
Benutzerdefinierte Aktionen für verschiedene Malware-Objekte (Spyware, Adware, Riskware, kostenpflichtige Dialer, Scherzprogramme)	■
Benutzerdefinierte Aktionen für infizierte und verdächtige Objekte: desinfizieren, in die Quarantäne verschieben, löschen	■
Benutzerdefinierte Aktionsfolge für Malware-Objekte, wenn die gegebene Aktion nicht vorgenommen werden kann	■
Auswahl von Aktionen für infizierte Pakete (Archive, Container, E-Mail-Dateien)	■
Prüfung archivierter Dateien mit beliebiger Rekursionstiefe	■
Prüfung	
Schnelles Scannen (Hauptspeicher, Bootsektoren aller Festplatten, Autostart-Objekte, Root-Verzeichnis der Boot-Platte, Windows-Root-Verzeichnis, Windows-Systemverzeichnis, Verzeichnis „Eigene Dateien", temporäres Systemverzeichnis, temporäres Benutzerverzeichnis)	■
Vollständiges Scannen (Prüfung aller lokalen Datenträger)	■
Heuristische Analyse	■
Die Nicht-Signatur-Technologie ergänzt die signaturbasierte Erkennung und die Heuristische Analyse	Origins Tracing™
Archive können vom Scannen ausgenommen werden	■
E-Mail-Dateien können vom Scannen ausgenommen werden	■
Schutz gegen Evasionstechniken	
Selbstschutz	Dr.Web SelfPROtect
Desinfektion	
Detektion und Neutralisierung von Viren, die mit unbekannten Packprogrammen gepackt wurden	FLY-CODE
Prüfung von Skripts einschließlich VB-Script und Java Script	■
Prüfung von Logical Values	■
Prüfung von E-Mail-Dateien	■
Detektion und Entfernung aktiver und passiver Schadsoftware folgender Spielarten: ■ Würmer ■ Rootkits ■ Datei-Viren ■ Trojaner ■ Dateilose Viren und Stealth-Viren ■ Plymorphe Viren ■ Malware und Makroviren, die MS Office Dateien infizieren ■ Skript-Viren ■ Spyware ■ Adware ■ Hackertools ■ Kostenpflichtige Dialer ■ Scherzprogramme	■
Aktualisierung	
On-Demand-Aktualisierung der **Dr.Web CureNet!** Virendatenbanken und Programm-Module via Internet	■
Größe der Virendatenbank	Optimierte Anzahl von Signaturen
Größe der Updates	Gering
Unterstützte Sprachen	
Benutzeroberfläche (Deutsch)	■
Benutzerhandbuch (Deutsch)	■
Support	
Kostenfreier technischer Support	■
Analyse unbekannter Viren	■

Dr.Web – Branchenführer bei der Desinfektion aktiver Infektionen

Ein wichtiger Gradmesser für die Effizienz eines Antivirenprogramms ist nicht nur seine Fähigkeit, Viren zu erkennen, sondern diese auch zu desinfizieren, verseuchte Dateien nicht nur zu löschen, sondern diese auch wiederherzustellen.

Die Funktionsfähigkeit auf einem bereits infizierten PC und eine ausschließliche Resistenz gegenüber Viren zeichnen Dr.Web unter anderen vergleichbaren Antivirenprogrammen aus.

- Branchenführer! Dr.Web verfügt über die höchste Desinfektionsrate bei aktiven Infektionen.
- Branchenführer! Dank einzigartigen Scantechnologien und hervorragenden Desinfektionsraten kann Dr.Web auf einem infizierten PC (ohne Vordesinfektion) installiert werden.

Antiviren-Engine

- Nur Dr.Web kann Archive mit beliebiger Rekursionstiefe vollständig überprüfen, eventuelle Bedrohungen erkennen und diese neutralisieren (selbst wenn Malware mehrfach mit verschiedenen Packprogrammen gepackt wurde).
- Dr.Web Technologien und Algorithmen ermöglichen es, gepackte Objekte mit geringster Fehlerquote zu detektieren, in einzelne Komponenten zu trennen und diese auf getarnte Bedrohungen hin zu analysieren. Selbst wenn Malware mit einer unbekannten Technik gepackt wurde, ist das Eindringen ins System völlig ausgeschlossen.
- Dr.Web ist ein Branchenprimus bei der Detektion und Neutralisierung von komplexen Viren wie MaosBoot, Rustock.C, Sector.
- Dank einzigartigen Technologien für die Prüfung des Hauptspeichers werden aktive Viren auf der Festplatte blockiert, bevor sie ihre Kopien erstellen. Das Risiko, dass Malware eine Sicherheitslücke in einer Anwendung bzw. im Betriebssystem findet, wird minimiert.
- Viren, die im Hauptspeicher aktiv und nicht als einzelne Dateien anzutreffen sind (z.B. Slammer und CodeRed), werden vom Dr.Web Antivirenprogramm detektiert und neutralisiert. Diesen Vorteil erhielt Dr.Web durch die Implementierung der Komplettüberprüfung des Systemspeichers. Im Juli 2001, als die CodeRed-Epidemie ausbrach, konnte das Virus nur von Dr.Web entdeckt werden. Auch heute können nur einige wenige Antivirenprogramme derartige Viren richtig desinfizieren.

Anti-Rootkit

- Der hocheffiziente Dr.Web Shield™ dient als sicherer Schutzschild, welcher das System gegen unsichtbare Rootkit-Viren abschirmt.
- Um Rootkits ausfindig zu machen, gewährt Dr.Web Shield™ dem Dr.Web Scanner einen privilegierten Zugriff auf Dateien, das Registry und kritische Systemkomponenten. Auf solche Weise werden Malware-Schutzmechanismen blockiert. Im Endeffekt werden alle bekannten Rootkit und Stealth-Viren detektiert.

Detektion unbekannter Bedrohungen

Das Dr.Web Know-how ermöglicht es, unbekannte Bedrohungen zu entdecken und zu blockieren. Ihre Daten werden permanent und sicher geschützt.

- FLY-CODE ist eine neue und einzigartige Technologie für die universale Entpackung, die im Dr.Web Suchmodul 5.0 implementiert wurde. Das Tool ermöglicht die Entpackung unbekannter Packformate. Das Suchmodul kann anhand jeweiliger Virensignaturen die Heuristische Analyse der Archive durchführen und bei Malware-Fund „Eventuell Trojan.Packed" in den Namen eines entdeckten Objektes hinzufügen.
- Eine hohe Erkennungsrate bei unbekannten Viren wird durch die Nicht-Signatur-Suche Origins Tracing™ erzielt. Dieses Tool hat seine Effizienz mehrmals während großer Epidemien, in denen Benutzer anderer Antivirenprogramme zu Schaden kamen, erfolgreich bewiesen. Origins Tracing™ ergänzt die herkömmliche Signatursuche sowie die Dr.Web Heuristik und erhöht dadurch die Detektionsrate bei unbekannter Schadsoftware. Durch Origins Tracing™ konnte die Anzahl von Signaturen in der Dr.Web Virendatenbank wesentlich verringert werden. Die Fehlerquote der Heuristischen Analyse konnte ebenfalls minimiert werden.
- Die Dr.Web Heuristik erkennt die meist verbreiteten Bedrohungen, indem sie diese klassifiziert und nach bestimmten Malware-Merkmalen einstuft. Selbst wenn eine bestimmte Signatur fehlt, wird der Malware ein Riegel vorgeschoben.

Selbstschutz

Dr.Web SelfPROtect macht das Antivirenprogramm immun gegen jegliche Evasionstechniken.

- Dr.Web SelfPROtect ist im Programm als Treiber implementiert und funktioniert auf der niedrigsten Ebene. Das Entladen bzw. Abbrechen des Treibers ist vor dem Neustart des Systems unmöglich.
- Dr.Web SelfPROtect schränkt den Malware-Zugriff auf das Netzwerk, Dateien und Verzeichnisse, Registry-Zweige und Wechseldatenträger ein und unterbindet jegliche Evasionstechniken.
- Im Vergleich zu einigen Konkurrenzprodukten, die den Windows-Kernel modifizieren (Unterbrüche überwachen, Vektortabellen unterschieben, nicht verifizierte Funktionen verwenden, usw.), ist das Selbstschutz-Modul Dr.Web SelfPROtect absolut eigenständig. Solche Modifikationen können schwerwiegende Funktionsprobleme des Betriebssystems bewirken und neue Sicherheitslücken öffnen.

Dr.WEB®
CureNet!

Desinfektion für Netzwerke in Extremfällen

Zentrale Desinfektion von Windows-Workstations und Servern in lokalen Netzwerken jeder Größenordnung per Fernzugriff (auch bei installierter Antivirensoftware eines anderen Herstellers)

http://products.drweb-av.de/curenet
http://www.drweb-curenet.com
http://www.drweb-av.de

Keine Viren in Ihrem Netzwerk? Sind Sie sicher?

Stellen Sie Ihre Antivirensoftware mit Dr.Web CureNet! auf die Probe!

Viele Unternehmen, die hohe Anforderungen an ihre IT-Sicherheit stellen, verwenden Antivirenprogramme verschiedener Hersteller, um Workstations, Server und Gateways in Ihrem Unternehmensnetzwerk zu schützen.

Wenn Sie an der Effizienz Ihrer Antivirensoftware zweifeln, nutzen Sie **Dr.Web CureNet!**. Die Installation des Programms sowie die Deinstallation der bereits installierten Antivirensoftware ist dabei nicht erforderlich. Sie können alle Rechner im Netzwerk prüfen und diese bei Bedarf desinfizieren.

Dr.Web CureNet! hilft, wenn andere versagen.

Profil

Produkt	**Dr.Web CureNet!**
Einsatzzweck	1. Zentrale Prüfung und Desinfektion von Workstations und Servern unter Windows, wenn die Antivirensoftware eines anderen Herstellers versagt. 2. Qualitätstest für das Antivirenprogramm eines anderen Herstellers.
Produktbeschreibung	http://products.drweb-av.de/curenet/
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"?	„Mein Dr.Web" ist ein persönlicher Bereich, in dem sich innerhalb der ganzen Lizenzlaufzeit Ihr persönlicher Link zum aktuellen Download befindet. Aus dem persönlichen Bereich kann sich der Abonnent mit dem technischen Support in Verbindung setzen, eine verdächtige Datei zur Analyse einreichen und weitere Services benutzen.
Lizenzierung	Das Tool wird nach Anzahl zu schützender Workstations (mindestens 5) für 1, 2 oder 3 Jahre lizenziert.
Demoversion	**Dr.Web CureNet!** ist nicht nur die Erste-Hilfe-Lösung. Es kann vom Administrator auch als Diagnosetool eingesetzt werden. Die kostenfreie Demoversion ermöglicht es, PCs im Netzwerk jederzeit zu prüfen und sicherzustellen, dass die installierte Antivirensoftware Malware detektiert. Die Funktion der Desinfektion ist in der Demoversion nicht verfügbar. Demoversion jetzt anfordern! http://download.drweb-av.de/demoreq/
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: mindestens 360 MB ■ HDD: mindestens 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: mindestens 360 MB ■ HDD: mindestens 200 MB
Kaufen	Bei Partnern http://partners.drweb-av.de oder im Online-Shop http://estore.drweb-av.de.

Vorteile

Einhaltung der sicherheitspolitischen Vorgaben

Für **Dr.Web CureNet!** sind kein Server und keine zusätzliche Software erforderlich. Das Netzwerk-Tool stört die Geschäftsabläufe nicht und ist mit der Sicherheitspolitik des Servers kompatibel. Die Dr.Web Scanner für Windows werden auf benutzerdefinierten Workstations verbreitet. Nach der Prüfung werden alle Scanner vollständig entfernt. **Dr.Web CureNet!** kann auch von einem USB-Datenträger aus gestartet werden.

Keine Internetverbindung erforderlich

Dr.Web CureNet! kann auch von USB-Datenträgern aus in isolierten Netzwerken gestartet werden. Die Verbreitung der Scanner, die Prüfung von Workstations und die Statistikerhebung hängen nicht von der DSL-Verbindung ab. Die Prüfung kann auch in Netzwerken erfolgen, die keine Internetverbindung haben.

Komplett vertraulich

Der Einsatz von **Dr.Web CureNet!** erfordert keine besonderen Vorkenntnisse. Die Oberfläche des **Dr.Web CureNet!** Assistenten führt den Administrator Schritt für Schritt und ist intuitiv verständlich. Der Administrator kann Scanvorgänge in Echtzeit überwachen. Nach der Desinfektion wird auf dem PC mit dem **Dr.Web CureNet!** Assistenten ein Protokoll über die von **Dr.Web CureNet!** vorgenommenen Aktionen gespeichert.

Immer aktuell

Der Link zu Ihrem persönlichen Download befindet sich innerhalb der ganzen Lizenzlaufzeit in Ihrem persönlichen Bereich „Mein Dr.Web". Unter diesem Link können Sie jederzeit eine aktuelle Version von **Dr.Web CureNet!** herunterladen. Sie können auch das Aktualisierungsmodul starten und frische Updates der **Dr.Web CureNet!** Virendatenbank laden.

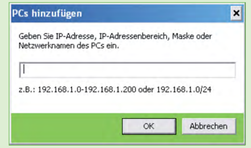
Wie funktioniert es? Ganz einfach

A. Laden Sie **Dr.Web CureNet!** aus Ihrem persönlichen Bereich "Mein Dr.Web" herunter.

B. Der Download verfügt über aktuelle Updates der Virendatenbank. Wenn Sie **Dr.Web CureNet!** das nächste Mal nutzen wollen, denken Sie bitte daran, dass **Dr.Web CureNet!** und die Virendatenbank aktualisiert werden sollten.

C. Die Suche nach Workstations und das Starten der Dr.Web Scanner für Windows auf definierten Rechnern werden mit dem **Dr.Web CureNet!** Assistenten per Fernzugriff durchgeführt. Der Assistent ist eine Windows-Applikation, die auf jedem PC mit einer Netzwerkverbindung installiert werden kann. Die Verbindung zum Rechner wird anhand der Rechte eines aktuellen Benutzers bzw. der Passwortliste für Workstations in diesem Netzwerk hergestellt.

D. Der Assistent überprüft das Netzwerk auf verfügbare Workstations, bevor die Virenscanner verbreitet werden. Sie können verfügbare Rechner prüfen oder Workstations und Server definieren, die auf Viren geprüft werden sollen. Die Rechner werden nach IP-Adresse, IP-Adressenbereich, Maske oder NetBIOS-Namen ausgewählt.

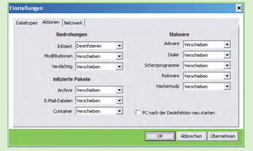


Dr.Web CureNet! ist jetzt bereit, Ihr Netzwerk zu prüfen und zu desinfizieren!

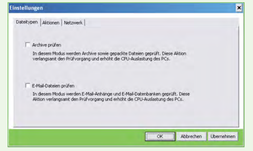
Prüfung und Desinfektion

Es gibt zwei Scanmodi: schnelles und vollständiges Scannen. Mit einem der Scanmodi kann die erforderliche Scantiefe definiert werden. In den meisten Fällen sind die Default-Einstellungen eine optimale Wahl.

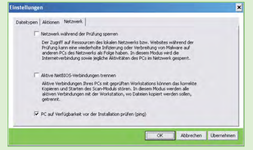
Die Reaktion des Scanners auf verschiedene Ereignisse kann individuell konfiguriert werden.



Um den Scanprozess zu beschleunigen, können Sie die Prüfung von Archiven und E-Mail-Dateien deaktivieren. Verdächtige Objekte werden in die Quarantäne verschoben. Die Quarantäne befindet sich auf dem PC mit dem installierten **Dr.Web CureNet!** Assistenten.

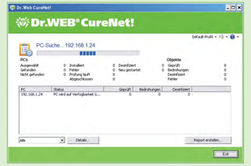


Um eine wiederholte Infizierung mit Netzwerk-Würmern zu vermeiden, können Sie die Netzwerkverbindung von Workstations ausschalten. Diese Funktion ist auf PCs mit dem installierten Assistenten nicht verfügbar.



Die Scan-Einstellungen können in XML-Profilen gespeichert werden. Sie können das Default-Profil benutzen bzw. Ihr eigenes Profil definieren.

Nachdem die Prüfung gestartet wurde, kann der Scanfortschritt in Echtzeit in der Statistiktabelle des **Dr.Web CureNet!** Assistenten eingesehen werden.



Nach der Prüfung wird ein Report erstellt.