Brauchen Sie einen guten Virenschutz?

Wir haben Dr.WEB®
seit 1992

Inhaltsverzeichnis

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 Malware-Detektion auf. Seit der Gründung des Unternehmens im Jahre 2003 wurde ein rapides Verkaufswachstum sowohl in Russland als auch in anderen Ländern erreicht.

Heute ist Doctor Web ein erfolgreiches und sich intensiv entwickelndes Unternehmen, das eine führende Rolle am Markt für IT-Sicherheit spielt. 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. Die Entwicklung neuer technologischer Lösungen, die Anwendern bei der Bekämpfung von beliebigen Virenbedrohungen helfen sollen, spielt auch eine wichtige Rolle. Die Produktpalette von Doctor Web umfasst eine große Anzahl an 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 die Dr.Web Antivirensoftware.

Dr.Web Technologien

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

Doctor Web ist einer der wenigen Anbieter weltweit, der über hauseigene Technologien für Detektion und Desinfektion von Malware verfügt. Das Unternehmen unterhält einen Virenüberwachungsdienst und ein analytisches Virenlabor. So können die Sicherheitsspezialisten blitzschnell auf neue Virenbedrohungen reagieren und Problemlösungen 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.

Technologien

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

Desinfektion von Viren

- Dr.Web läuft auf einem bereits infizierten PC und verfügt über eine außergewöhnliche Virenresistenz.
- Dr.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 des bereits installierten Antivirenprogramms).
- Starten der Prüfung auf einem infizierten PC 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 Registry-Zweige 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 Betriebssystems bewirken kann und neue Sicherheitslücken öffnet, läuft Dr.Web SelfPROtect vollständig autonom.

Einzigartige Möglichkeiten der Engine

- Prüfung von Archiven mit beliebiger Rekursionstiefe.
- Entdeckung gepackter böswilliger Objekte mit hoher Genauigkeit und Analyse einzelner Komponenten auf versteckte Bedrohungen.
- Dr.Web ist Branchenführer bei der Entdeckung und Beseitigung komplexer Viren wie MaosBoot, Rustock.C oder Sector.
- 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.
- Detektion und Neutralisierung 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 noch nicht eingetragene Bedrohungen entdeckt werden können.
- Durch Dr.Web Heuristik werden alle verbreiteten Virenbedrohungen entdeckt und nach ihren jeweiligen Kennungen klassifiziert.

Technologien der Spam-Filterung

Dr.Web Antispam analysiert E-Mails anhand mehrerer tausend Regeln, die in mehrere 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

  Die Filterung von Evasions-Techniken ist eine der fortschrittlichen und effizienten Dr.Web Antispam-Technologien. Sie erkennt verschiedene Evasions-Techniken, die Spammer zur Umgehung von Antispam-Filtern verwenden.
- Analyse anhand von 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.
- Detektion von Spam nach E-Mail-Adressen

  Die Detektion 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

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

  So genannte 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 weder trainiert noch konfiguriert zu werden. Im Vergleich zu Antispamprogrammen, welche die Bayes'sche Analyse verwenden, ist Dr.Web Antispam nicht lernbedüftig und startet die Bearbeitung mit dem Eingang der ersten E-Mail. So ist für Dr.Web Antispam eine tägliche Administration nicht erforderlich.
- Keine Verlangsamung der E-Mail-Zustellung.
- Filterung von E-Mails in Echtzeit.
- Hohe Filterungsgeschwindigkeit bei geringen Systemanforderungen.
- Bearbeitung von Objekten beliebiger Rekursionstiefe.
- 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 hat im Vergleich zu anderen Antivirenprogrammen eine sehr kleine Virendatenbank. Dies ist der auf einer flexiblen Sprache basierenden hauseigenen Technologie zu verdanken, die für die Dr.Web Virendatenbank gedacht ist. Eine kleine Virendatenbank sorgt für einen geringen Internet-Verkehr und beansprucht weniger Platz auf der Festplatte und im Hauptspeicher. Dadurch können 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 vermitelt uns jedoch keine Vorstellung darüber, wie viele Viren von einem Antivirenprogramm erkannt und beseitigt werden können. Um zu begreifen, warum die Anzahl von Signaturen in der Dr.Web Virendatenbank geringer 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.

Was bringt dem Anwender eine kleine Größe der Dr.Web Virendatenbank und eine geringe Anzahl an Virensignaturen?

- Geringer Platzbedarf auf der Festplatte.
- 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, entwickelt Virensignaturen und veröffentlicht Updates nach der Analyse jeder neuen Bedrohung (in der Regel mehrmals pro Stunde).
- Nach der Veröffentlichung sind alle Updates auf mehreren Servern in verschiedenen Regionen der Welt verfügbar.
- Um Fehler bei der Detektion 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.

Dr.Web Enterprise Security Suite

Produkte für Business

Dr.Web Enterprise Security Suite: Produkte für Business

Dr.Web Enterprise Security Suite ist ein Gesamtpaket von Dr.Web Produkten, welches sämtliche Schutzwerkzeuge für alle Computer Ihres Unternehmensnetzwerks und ein einheitliches Verwaltungscenter für die meisten Computer enthält. Die Produkte lassen sich in 5 Gruppen einteilen. Dies erleichtert die Suche nach einem passenden Produkt.

Kommerzielles Produkt	Software-Produkt
Dr.Web Desktop Security Suite Schutz für Workstations sowie Clients von Terminalservern, virtuellen Servern und integrierten Systemen	Dr.Web für Windows
	Dr.Web KATANA
	Dr.Web für Linux
	Dr.Web für macOS
	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 macOS Server
	Dr.Web für Novell Storage Services
	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 Mac*
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 Microsoft ISA Server und Forefront TMG
	Dr.Web für MIMEsweeper
	Dr.Web für Qbik WinGate
Dr.Web Mobile Security Suite Schutz für mobile Endgeräte	Dr.Web für Android
	Dr.Web für BlackBerry

* Wird momentan entwickelt.

Lizenzierung von Dr.Web Enterprise Security Suite

Die Lizenzierung für jedes Produkt erfolgt separat. Für den Schutz eines jeden Objektes müssen Sie eine Basislizenz und bei Bedarf zusätzliche Komponenten auswählen.

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 10/8/8.1/7/Vista SP2/XP SP2+ (32 und 64 Bit).	Rundumschutz	■ Verwaltungscenter
	Windows 10/8/8.1/7/Vista SP2 (64-Bit).	Antivirus	
	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 und 64 Bit).	KATANA	■ Verwaltungscenter
	Windows 10/8/8.1/7/Vista SP2 (64-Bit).		
	Linux glibc 2.7 and later	Antivirus	■ Verwaltungscenter
	macOS 10.7 and later		
	MS-DOS OS/2		
Dr.Web Server Security Suite Dateiserver Anwendungsserver Terminalserver Virtuelle Server	Windows	Antivirus	■ Verwaltungscenter
	Novell NetWare		
	macOS Server		
	Unix (Samba)		
Dr.Web Mail Security Suite E-Mail-Anwender	Unix	Antivirus	■ Verwaltungscenter ■ Antispam ■ SMTP-Proxy
	MS Exchange		
	Lotus (Windows/Linux)		■ Antispam ■ SMTP-Proxy
	Kerio (Windows/Linux)		■ SMTP-Proxy
Dr.Web Gateway Security Suite Anwender von Internet-Gateways	Internet gateways Kerio (Windows/Linux)	Antivirus	
	Internet gateways UNIX		■ Verwaltungscenter
	Qbik WinGate		
	MIMEsweeper		■ Antispam
	Microsoft ISA Server and Forefront TMG		
Dr.Web Mobile Security Suite Mobile Endgeräte	Android OS 4.0–7.1	Rundumschutz	■ Verwaltungscenter
	BlackBerry		

Universalität

Für die vom Kunden gewünschte Lösung wird eine Dr.Web Schlüsseldatei für alle zu schützenden Objekte erstellt. Der Schlüssel umfasst auch Dr.Web Produkte für ein beliebiges Objekt für alle Betriebssysteme und Plattformen, die von Dr.Web unterstützt werden.

Nützliche Links

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

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 einzigen Arbeitsplatz aus (Web-Administration).
- Minimale Gesamtkosten im Vergleich zu Konkurrenzprogrammen durch die Möglichkeit der Einrichtung eines Netzwerks unter Windows- und UNIX-Servern.
- Einfache Installation und sicherer Schutz.
- Das Schutzsystem kann unabhängig von der Größe und den Besonderheiten (Anzahl der Mitarbeiter, 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-Scripts, Remote-Installation. Die Installation ist auch dann möglich, wenn ein Computer für den Antivirus-Server nicht erreichbar ist.
- Einstellung individueller Sicherheitsvorgaben für Unternehmen und einzelne Mitarbeitergruppen.
- Automatisierung durch Integration mit Windows Network Access Protection (NAP).
- Variable 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.
- Die Protokollierung der 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 breit verzweigten Filialstruktur verwendet werden.
- Die Konfiguration von Sicherheitsvorgaben für verschiedene Benutzertypen (u.a. mobile Benutzer) und Workstations trägt zum aktuellen Stand des Schutzsystems bei.
- Die selbständige Anpassung der Schutzparameter ist aus Sicherheitsgründen unmöglich.
- Schutz für Netzwerke ohne Internetverbindung.
- 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 Scriptsprache. Dies ermöglicht einen direkten Zugriff auf interne Oberflächen des Verwaltungscenters.
- Zurücksetzen von Updates, auch wenn der Update-Vorgang einen Fehler hervorruft. Der Netzwerk-Knoten bleibt trotz alledem geschützt.
- 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.

Nützliche Links

Produktbeschreibung:
http://products.drweb-av.de/enterprise_security_suite/control_center

Dr.Web Desktop Security Suite

Virenschutz für Workstations, Clients von Terminalservern und integrierte Systeme

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

Lizenzierung

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

Software-Produkte der Gruppe Dr.Web Desktop Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im zweiten Fall wird das Verwaltungscenter von Dr.Web Enterprise Security Suite (außer bei Dr.Web Konsolen-Scanner) zusätzlich lizenziert.

Lizenzvarianten

	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 Bit) **Windows 10/8/8.1/7/Vista SP2 (64 Bit)**		**Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 Bit)** **Windows 10/8/8.1/7/Vista SP2 (64 Bit)**	**Linux**	**macOS**	**MS DOS, OS/2**
Basislizenz	Rundumschutz	Antivirus	KATANA	Antivirus		
Schutzkomponente der Basislizenz	■ Antivirus ■ Antispyware ■ Antirootkit ■ Antispam ■ Web-Antivirus ■ Office Control ■ Firewall	■ Antivirus ■ Antispyware ■ Antirootkit ■ Firewall	■ Nicht-Signatur-Antivirensoftware ■ Dr.Web Cloud ■ Verwaltungscenter	■ Antivirus ■ Antispyware	■ Antivirus ■ Antispyware ■ Antirootkit	■ Antivirus ■ Antispyware ■ Antirootkit
Zusätzliche Schutzkomponenten						
Verwaltungscenter	+	+	+*	+	+	–

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

Unterstützte Betriebssysteme

Dr.Web für Windows	Dr.Web für Linux	Dr.Web für macOS	Dr.Web Konsolen-Scanner
Rundumschutz, Antivirus: Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 und 64 Bit). Windows 10/8/8.1/7/Vista SP2 (64-Bit). **KATANA:** Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 und 64 Bit). Windows 10/8/8.1/7/Vista SP2 (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)	macOS 10.7 und höher	Windows, MS DOS, OS/2

Dr.Web Antivirus für Windows

Minimal erforderlicher Viren- und Spywareschutz für PCs und Laptops

Vorteile

- Branchenführer bei der Desinfektion aktiver Vireninfektionen.
- Möglichkeit der Installation auf einem infizierten Computer ohne vorherige Desinfektion des bereits installierten Antivirenprogramms.
- Einzigartige Technologie für die Blockierung unbekannter Bedrohungen (Origins Tracing).
- Komplettprüfung von Archiven beliebiger Rekursionstiefe.
- Branchenführer bei der Erkennung und Beseitigung komplexer Viren wie MaosBoot, Rustock.C oder Sector.
- Schutz vor unerlaubten Zugriffen von außen, Vorbeugen von Datenverlusten, Blockierung von verdächtigen Verbindungen auf Paket- und Anwendungsebene (im Falle von Lizenzen, die eine Firewall beinhalten).

Schutzkomponenten der Basislizenz

- Antivirus.
- Antispyware.
- Antirootkit.
- Firewall.

Lizenzvarianten

- Antivirus.
- Rundumschutz*.

Systemanforderungen

Unterstützte Betriebssysteme

- Windows 8.1/8/7/Vista/XP (32 und 64 Bit).

HDD

- Mindestens 450 MB für die Installation aller Dr.Web Komponenten.

Nützliche Links

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

Auf Version mit einer Firewall umsteigen:
http://promotions.drweb-av.de/upgrade/security_space

* Nur für Windows 8.1/8/7/Vista/XP (32 und 64 Bit).

Dr.Web Antivirus für macOS

Minimal erforderlicher Schutz vor Viren und sonstigen schädlichen Objekten, die nicht nur macOS, sondern auch andere Betriebssysteme angreifen

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.

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 dann möglich, wenn zuvor gewählte Aktionen nicht durchführbar waren).
- Auf Anforderung Auslassen bestimmter Pfade und Dateien bei der Überprüfung.
- 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 Kommandozeilen-Tools, Möglichkeit der Integration von Modulen in Apple Scripts-Systeme.

Systemanforderungen

- macOS 10.7 und höher (32 und 64 Bit).
- Internetverbindung: Registrierung und Herunterladen von Updates.

Nützliche Links

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

Dr.Web Antivirus für Linux

Minimal erdorderlicher Virenschutz

Vorteile

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

Schlüsselfunktionen

- Erkennung und Neutralisierung von Malware und schädlichen Objekten auf Festplatten und Wechseldatenträgern.
- Erkennung von Viren in Archiven beliebiger Rekursionstiefe und gepackten Objekten.
- Prüfung von Dateien, die durch bekannte sowie unbekannte Packprogramme komprimiert wurden, via FLY-CODE™.
- 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 den Optionen Wiederherstellung und Einschränkung der Quarantäne-Größe.
- Erstellen von Statistiken.
- Automatisches Update nach Zeitplan und auf Anforderung.

Systemanforderungen

- Plattform: Intel x86/amd64.
- HDD: Mindestens 400 MB.
- Betriebssystem: GNU- und Linux-Distributionen mit Kernel 2.6.x.
- Internetverbindung: Registrierung und Herunterladen von Updates.

Nützliche Links

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

Dr.Web Konsolen-Scanner

Virenschutz mit erweiterten Automatisierungsmöglichkeiten für fortgeschrittene Anwender

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 auf Embedded-Systemen und können sogar leistungsschwache Computer sicher schützen.
- Komfortable Prüfung: Der Administrator kann die Prüfung manuell oder auch nach Zeitplan durchführen.
- Desinfektion der von Viren befallenen Workstations und Server (u.a. außerhalb des Netzwerks).
- Hohe Virenresistenz und Möglichkeit der Installation auf einem 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/

Dr.Web Server Security Suite

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

- Dr.Web für Windows-Server
- Dr.Web für Novell NetWare-Server
- Dr.Web für UNIX (Samba)-Server
- Dr.Web für macOS-Server
- Dr.Web für UNIX (Novell Storage Services)-Server

Lizenzierung

Software-Produkte der Gruppe Dr.Web Server Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im zweiten Fall wird das Verwaltungscenter von Dr.Web Enterprise Security Suite (außer bei Dr.Web für Server UNIX) zusätzlich lizenziert.

Lizenzvarianten

Dr.Web für Windows-Server	Dr.Web für Novell NetWare-Server	Dr.Web für macOS-Server	Dr.Web für UNIX (Samba)-Server	Dr.Web für UNIX (Novell Storage Services)-Server
Basislizenz: Antivirus				
Zusätzliche Komponenten: Verwaltungscenter				
+	+	+	+	+

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

Unterstützte Betriebssysteme

Dr.Web für Windows-Server	Dr.Web für Novell NetWare-Server	Dr.Web für macOS-Server	Dr.Web für UNIX (Samba)-Server	Dr.Web für UNIX (Novell Storage Services)-Server
Microsoft Windows Server 2000* / 2003 (x32 und x64*) / 2008 / 2012 (x64)	Novell NetWare 4.11-6.5 mit den installierten Erweiterungen aus der Minimum patch list	macOS Server 10.7 und höher	Distributionen mit Linux-Kernel 2.6.x (32 und 64 Bit)	Unterstützte Betriebssysteme: SUSE Linux, Enterprise Server, 10 SP3

* Unterstützung nur für Version 7.0.

Dr.Web für Windows-Server

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 dem 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.
- 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 Serververbänden 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 Löschung der in die Quarantäne verschobenen Objekte.
- Protokollierung von Aktionen des Programms.
- Automatisches Update der Virendatenbanken.
- Schonende Systemanforderungen und Berücksichtigung der Systemleistung.
- Dr.Web Cloud: Blitzschnelle Reaktion auf neue Bedrohungen*.
- Der proaktive Virenschutz bietet einen zuverlässigen Schutz vor unbekannten Bedrohungen durch die Blockierung der Modifikation kritischer Windows-Dateien und die Überwachung von sicherheitsgefährdenden Aktionen*.

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.

Dr.Web für Novell NetWare-Server

Virenschutz für Datenlager

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 der zu prüfenden Objekte sowie der entsprechenden Aktion für entdeckte Viren oder verdächtige Dateien).

Schlüsselfunktionen

- Prüfung von Serververbänden nach Zeitplan oder auf Anforderung des Administrators.
- Prüfung sämtlicher Dateien, die durch den Server übertragen werden „on the fly".
- Parallele Prüfung mehrerer Dateien.
- Regelung der Serverauslastung und Einstellung der Scanpriorität im System.
- Automatische Trennung der Verbindung vom Server zum PC (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.

Systemanforderungen

- Novell NetWare 4.11-6.5 mit installierten Erweiterungen aus der Minimum Patch List.
- 25 MB Hauptspeicher + 25 MB Hauptspeicher für jeden weiteren Scanprozess.
- HDD: 20 MB.

Nützliche Links

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

Dr.Web für macOS-Server

Virenschutz für Workstations unter Server-Versionen macOS

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.

Schlüsselfunktionen

- Prüfung von Autostart-Dateien, Wechseldatenträgern, Netzwerk-Treibern und Logical Values, E-Mails sowie Dateien und Verzeichnisse (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 Desinfektion, Verschiebung in die Quarantäne und Entfernung (auch dann, wenn die früher ausgewählte Aktion nicht durchführbar war).
- Auslassen bestimmter Pfade und Dateien bei der Überprüfung auf Anforderung.
- Erkennen und Löschen von Viren, die durch unbekannte Packprogramme gepackt wurden.
- Protokollierung des Zeitpunktes eines Ereignisses, des geprüften Objektes und der durchgeführten Aktion.
- Automatisches Update der Virendatenbanken und der 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 Löschung der in die Quarantäne verschobenen Objekte.
- Detaillierte Protokollierung.
- Verwendung von Modulen als Tools der Kommandozeile, Möglichkeit der Integration von Modulen in Apple Scripts-Systeme.

Systemanfoderungen

- macOS 10.7 oder höher.
- Prozessor Intel.
- Hauptspeicher: 128 MB.
- HDD: 120 MB.
- Internetverbindung: Registrierung und Herunterladen von Updates.

Nützliche Links

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

Dr.Web für UNIX (Samba)-Server

Virenschutz für Datenlager

Vorteile

- Hohe Leistungsfähigkeit und Funktionsstabilität.
- Hoher Durchsatz des Scanners bei minimaler Auslastung des Betriebssystems. Dr.Web funktioniert deshalb auf Servern beliebiger Konfiguration einwandfrei.
- 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).
- Einfache Installation, Konfiguration und Administration.

Schlüsselfunktionen

- Prüfung von Serververbänden nach Zeitplan oder auf Anforderung des Administrators.
- Prüfung „on the fly" während der Speicherung oder Öffnung von Dateien auf dem Server von Workstations aus.
- Parallele Prüfung mehrerer Dateien.
- Automatische Trennung der Verbindung vom Server zur Workstation, sofern einer von beiden Quelle einer Virenbedrohung ist.
- Blitzschnelle Benachrichtigung des Administrators, anderer Benutzer und Benutzergruppen über Virenfunde 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.

Systemanfoderungen

- Dr.Web Daemon (drwebd) 5.0 und höher.
- Samba 3.0 und höher.

Unterstützte Betriebssyteme

- Distributionsdatei Linux mit Kernel ab Version 2.4.x.
- FreeBSD ab Version 6.x für Intel x86-Plattform und amd64.
- Solaris 10 für die x86-Plattform Intel und amd64.

Nützliche Links

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

Dr.Web für UNIX (Novell Storage Services)-Server

Virenschutz für Datenspeicher

Vorteile

- Hohe Leistung und Funktionsstabilität.
- Hoher Scan-Durchsatz bei minimaler CPU-Auslastung. So kann Dr.Web für Novell Storage Services auf Servern beliebiger Konfiguration einwandfrei funktionieren.
- Flexible Konfiguration (Auswahl der zu prüfenden Objekte und Aktionen gegenüber gefundenen Viren und verdächtigen Objekten).
- Hervorragende Kompatibilität (keine Konflikte mit bekannten Firewalls und Datei-Wächtern).
- Bequeme Administration.
- Leichte Installation und Konfiguration.

Schlüsselfunktionen

- Desinfektion oder Löschung beliebiger schädlicher Objekte.
- Asynchrone Prüfung (beim Speichern oder Öffnen von Dateien auf dem Server über Workstations).
- Parallele Prüfung mehrerer Dateien.
- Zentrale Sammlung von Statistiken, die sämtliche Systemfunktionen betreffen.
- Benachrichtigung des Administrators über Ergebnisse der Prüfung per E-Mail.
- Verschiebung infizierter und verdächtiger Dateien in die Quarantäne. Desinfektion, Wiederherstellung und Löschung von Dateien aus der Quarantäne. Protokollierung von Aktionen. Schutz eigener Module vor Evasions-Techniken.
- Automatisches Update der Virendatenbanken.

Systemanfoderungen

- Novell Open Enterprise Server SP2 auf Basis von SUSE Linux Enterprise Server 10 SP3.
- Installierte Novell Storage Services (NSS).
- NSS-Dateisystem im Systemverzeichnis.
- 300 MB Freiplatz auf der Festplatte für die Installation des Produktes.

Nützliche Links

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

Dr.Web Mail Security Suite

E-Mail-Schutz

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

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).

Software-Produkte der Gruppe Dr.Web Mail Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden.Im zweiten Fall wird das Verwaltungscenter von Dr.Web Enterprise Security Suite, Antispam und SMTP-Proxy zusätzlich lizenziert.

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.

Lizenzvarianten

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

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

Unterstützte Betriebssysteme

Dr.Web Produkt	Windows	macOS	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		Red Hat Enterprise Linux (RHEL) 4, 5 und 6, Novell SuSE Linux Enterprise Server (SLES) Versionen 9, 10 und 11 (nur 32 Bit)		
Dr.Web für Mailserver Kerio	2000/XP/Vista/7, Server 2003/2008/2012	macOS 10.6 Snow Leopard, macOS 10.5 Leopard, macOS 10.4 Tiger.	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		

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 im Hinblick auf Viren und Spam.
- Analyse von E-Mails und ihren Komponenten.
- Korrekte Prüfung der meisten Archivformate (einschließlich mehrbändiger und selbstextrahierender Archive).
- White- und Blacklists.
- Konfigurierbare Benachrichtigung.
- Erhebung von Statistiken.
- Schutz von Programm-Modulen vor Ausfällen.

Dr.Web für Mailserver UNIX verfügt über Konformitätszertifikate des Föderalen Dienstes für technische Überwachung und Exportkontrolle sowie des Föderalen Sicherheitsdienstes. So können Dr.Web Sicherheitsprodukte in Unternehmen mit sehr hohen 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 allen gängigen Sicherheitsanforderungen und dem Datenschutzgesetz.

Geringer Administrationsaufwand

Trotz der Vielzahl verschiedener Funktionen erfordert Dr.Web für Mailserver UNIX keine komplizierte Konfiguration. Zusätzlich erfolgt die Lieferung von Dr.Web für Mailserver UNIX stets in Kombination mit Dr.Web Office Shield — einem Server, der nach der Installation keinerlei Wartung oder Pflege benötigt.

Schnelle Rückmeldung

Die Technologie der parallelen Prüfung mehrerer Dateien sorgt für eine schnelle Rückmeldung des Systems. Die Prüfung erfolgt „on the fly". Gleichzeitig werden weitere Dateien empfangen. So erhalten Endanwender trotz laufender Prüfung ihre E-Mails sekundenschnell.

Weitere Vorteile von Dr.Web Antispam:

- Ein Training des Produkts ist nicht erforderlich. Im Unterschied zu Antispam-Programmen, die auf der Bayes-Analyse basieren, funktioniert Dr.Web Antispam effizient 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 Detektionsfehlern.
- Update einmal täglich. 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 die Möglichkeit der Quarantäne-Verwaltung sowohl über die Web-Oberfläche als auch durch ein entsprechendes Tool. Darüber hinaus werden alle eingehenden E-Mails archiviert.

Einfache Administration

Die Verwendung der Web-Oberfläche zur Konfiguration und Verwaltung des Produktes ermöglicht eine leichte Konfiguration von jedem Ort dieser Welt aus.

Konfigurierbare Lösung

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

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 mittels der Dr.Web-Engine auf Viren prüft.
- Vaderetro ist ein Plug-in, das E-Mails auf Basis der Vade Retro-Bibliothek auf Spam filtert.
- Headersfilter ist ein Plug-in, das E-Mails nach Header-Informationen filtert.

Unterstützte Betriebssysteme

- Linux-Distributionsdateien mit Kernel 2.4.x und höher.
- FreeBSD 6.x und höher für die Plattform Intel x86.
- Solaris 10 für die Plattform Intel x86.

Nützliche Links

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

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 auch 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 Serverauslastung wird dadurch verringert. Ihre Mitarbeiter können sich auf die Arbeit konzentrieren, statt durch Spam abgelenkt zu werden.
- Filterung nach Black- und Whitelists: Bestimmte E-Mail-Adressen können von der Prüfung ausgeschlossen werden.
- Effektive Filterung nach Dateitypen.
- 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 parallele Prüfung mehrerer Dateien.
- Einzigartige Technologien zur Entdeckung bisher unbekannter Packprogramme und schädlicher 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: Definition der Maximalgröße der zu prüfenden Objekte, Auswahl von Aktionen (u.a. für Dateien, die nicht geprüft werden können) und Behandlungsmethoden für infizierte Objekte.
- Detektion schädlicher Objekte 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.
- Statistik.
- Automatisches Update.

Systemanfoderungen

HDD

- Microsoft Exchange Server 2000/2003/2007/2010: 512 MB.
- Microsoft Exchange Server 2013/2016: 1 GB.

Unterstützte Betriebssysteme

- Für MS Exchange Server 2000/2003: Microsoft Windows 2000 Server oder Advanced Server mit dem installierten SP4; Microsoft Windows Server 2003 (Standard, Enterprise oder Datacenter) mit dem installierten SP1 oder höher.
- Für MS Exchange Server 2007/2010: Microsoft Windows Server 2003 R2x64 mit dem installierten SP2; Microsoft Windows Server 2008 x64.
- Für Microsoft Exchange Server 2013/2016: Microsoft® Windows Server® 2008 R2; Microsoft® Windows Server® 2012; Microsoft® Windows Server® 2012 R2.

Nützliche Links

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

Dr.Web für Mailserver Kerio

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

Vorteile

- Hervorragende Kompatibilität mit Mailservern Kerio.
- Dr.Web bietet Ihnen das zur Zeit einzige Antivirus-Plug-in für Mailserver Kerio.
- Technischer Support.
- Minimale Zustellungszeit von E-Mails und hohe Zuverlässigkeit des Produktes durch die Technologie der parallelen Prüfung von Dateien.
- Minimale Systemanforderungen und keine Auslastung des lokalen Netzwerks.
- Flexible und clientorientierte Konfiguration: Auswahl der zu prüfenden Objekte und der entsprechenden, auszuführenden 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: Microsoft Windows 2000/XP/Vista/7, Microsoft Windows Server 2003/2008/2012 (32 und 64 Bit).
- Version für Linux: 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; Red Hat 9.0.
- Version für macOS: macOS 10.6 Snow Leopard, macOS 10.5 Leopard, macOS 10.4 Tiger.

Nützliche Links

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

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 funktioniert nicht nur auf einzelnen Servern, sondern auch auf Partitionsservern und Lotus Domino-Clustern. Dabei laufen autonome Kopien der Antivirenprogramme im PC-Speicher, welche 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 parallelen Prüfung mehrerer Dateien 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.
- Einfache Installation und flexible Konfiguration

  Die Einrichtung von Dr.Web für IBM Lotus Domino kann leicht automatisiert werden. Die vorhandene Unterstützung von Administrationsskripts ist ausführlich dokumentiert. Die flexible Konfiguration der Aktionsalgorithmen des Antivirenprogramms bei Scanergebnissen ermöglicht die Benachrichtigung des Absenders, Empfängers und Systemadministrators im Hinblick auf entdeckte Viren. E-Mail-Header und angehängte Dateien bleiben dabei erhalten.
- Bequeme Administration

  Die Gruppierung und Verwaltung von Gruppen vereinfachen die Administration des Virenschutzes. Für jede Gruppe können verschiedene Einstellungen definiert werden. Identische 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 (unter anderem anhand von Black- und Whitelists).
- Virenprüfung von Dateien in nsf-Datenbanken.
- Die Prüfung von Objekten auf Anforderung durch manuellen Start bzw. das Abbrechen von Aufgaben des Scanners ist jederzeit möglich.
- Analyse von E-Mails und Sortierung aller E-Mail-Komponenten zur weiteren Analyse.
- Desinfektion verseuchter E-Mails und angehängter Dateien.
- Detektion von Malware in mehrfach gepackten Dateien.
- Entdeckung von bösartigen Objekten, die durch unbekannte Packprogramme versteckt wurden.
- Entdeckung unbekannter bösartiger Objekte.
- Verschiebung infizierter und verdächtiger Objekte in die Quarantäne (der Zugriff auf die in die Quarantäne verschobenen Objekte erfolgt über den 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: Windows Server).
- Version für Linux: Red Hat Enterprise Linux (RHEL) 4, 5 und 6, Novell SuSE Linux Enterprise Server (SLES) 9, 10 und 11 (nur 32 Bit).

Nützliche Links

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

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 Microsoft ISA Server und Forefront TMG
- Dr.Web für Qbik WinGate
- Dr.Web für MIMEsweeper

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).

Software-Produkte der Gruppe Dr.Web Gateway Security Suite können separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im zweiten Fall wird 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) zusätzlich lizenziert.

Lizenzvarianten

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

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

Unterstützte Betriebssysteme

Dr.Web Produkt	Windows
Dr.Web für Internet-Gateways Kerio	2000/XP/ 2003/ 2008/ 7/ Vista
Dr. Web für Microsoft ISA Server und Forefront TMG	Bei der Verwendung von Microsoft ISA Server: Microsoft Windows Server 2003 x86 mit Service Pack 1 (SP1); Microsoft Windows Server 2003 R2 x86. Bei der Verwendung von Microsoft Forefront TMG: Microsoft Windows Server 2008 SP2; Microsoft Windows Server 2008 R2.
Dr.Web für MIMEsweeper	2000 Server SP4 oder höher/Server 2003 oder höher/ 2008.
Dr.Web für Qbik WinGate	Vista/Server 2008/Server 2003/XP/2000 (32 und 64 Bit).

Dr.Web Produkt	Linux	FreeBSD	Solaris
	Intel x86 / 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 UNIX

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

Vorteile

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

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 Systemfunktionen.
- Benachrichtigung des Benutzers über das Hochladen einer Malware-Webseite oder eines Virenfundes.

Unterstützte Betriebssysteme

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

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

- Squid ab 3.0.
- Shweby ab 1.0.
- SafeSquid ab 3.0.

Nützliche Links

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

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 mit der Kerio-Firewall kombinierbar ist. Das Plug-in wird auf dem Computer installiert und anschließend von Kerio als externe Antivirensoftware verwendet.

Vorteile

- Zuverlässiger Schutz für den Internetzugang von Privatanwendern und Unternehmen beliebiger Größe in beliebigen Branchen.
- Funktion im Modus des zentral verwalteten Schutzes durch das Verwaltungscenter von Dr.Web Enterprise Security Suite.
- Leichte Administration (Möglichkeit, über alle Virenereignisse via E-Mail oder SMS benachrichtigt zu werden).
- Minimale Zustellungszeit der E-Mails durch die parallele Prüfung mehrerer Dateien.

Schlüsselfunktionen

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

Systemanfoderungen

Für Windows:

- HDD: Mindestens 350 MB.
- Betriebssystem: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32 und 64 Bit)
- Mailserver: Kerio MailServer 6.2 oder höher, Kerio Control 7.0.0 – 7.4.2.

Für Linux:

- HDD: Mindestens 55 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.
- Mailserve: Kerio MailServer 6.2 oder höher, Kerio Connect 7.

Nützliche Links

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

Dr.Web für Microsoft ISA Server und Forefront TMG

Viren- und Spamprüfung der durch Microsoft ISA Server und Forefront TMG übertragenen Daten

Vorteile

- Prüfung beliebiger Objekte in kürzester Zeit durch eine dynamische Analyse des Ressourcen-Bedarfs anderer Server-Services und blitzschnelles Umschalten zwischen den Aufgaben.
- Neueste Plattformen für die Erhöhung des Scan-Durchsatzes.
- Funktion auf Servern beliebiger Konfiguration (u.a. mit geringem Hauptspeicher).
- Schutz für reelle und virtuelle Server.
- Das Antispam-Modul erfordert kein Training und funktioniert bereits ab dem ersten Programmstart einwandfrei. Die Serverauslastung wird dadurch verringert und die Mitarbeiter eines Unternehmens können sich auf ihre Arbeit statt auf Spam konzentrieren.
- Blockierung des Zugriffs auf bestimmte Inhalte und Filterung nach Dateityp. Das Einschleusen von Malware ist dadurch ausgeschlossen.
- Einzigartige Technologien zur Entdeckung neuester Packprogramme und böswilliger Objekte.
- Installation und Feineinstellung nach Unternehmensbedarf.
- Ausführliche Dokumentation.

Schlüsselfunktionen

- Viren- und Spamprüfung der gesamten übertragenen Daten (u.a. angehängte Dateien).
- Prüfung von Dateien „on the fly" und Entdeckung schädlicher Objekte in mehrfach gepackten Dateien.
- Desinfektion infizierter Dateien.
- Verschiedene Aktionen je nach Spam-Art.
- E-Mails, die Sicherheitsbedrohungen enthalten, werden mitsamt einem warnenden Begleittext gesendet.
- Einschränkung des Zugriffs auf infizierte Daten für alle Benutzer lokaler Netzwerke.
- Einschränkung des Zugriffs auf Internet-Inhalte durch das Office-Control-Modul.
- Verschiebung infizierter und verdächtiger Dateien in die Quarantäne.
- Benachrichtigung des Administrators über Viren-Ereignisse.
- Protokollierung.
- Automatische Updates.

Lizenzierung

Lizenztyp

- Nach Anzahl der zu schützenden Anwender (unbegrenzt).
- Pro geschütztem Server für die Prüfung des unbegrenzten E-Mail-Volumens auf einem Server mit bis zu 3000 zu schützenden Anwendern.

Lizenzvarianten

- Antivirus.
- Antivirus + Antispam.
- Auch Microsoft ISA Server und Forefront TMG ist im kostengünstigen Dr.Web Small Business Bundle verfügbar.

Systemanfoderungen

Für Microsoft ISA Server:

- Prozessor: Pentium III 733 MHz und höher.
- Hauptspeicher: 1 GB und größer.
- HDD: 300 MB für die Installation. Der zusätzliche Freiplatz auf der Festplatte ist für temporäre Daten während der Virenprüfung erforderlich.
- 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:

- Prozessor: Pentium III 1.86 GHz und höher.
- Hauptspeicher: 2 GB und größer.
- HDD: 300 MB für die Installation. Der zusätzliche Freiplatz auf der Festplatte ist für temporäre Daten während der Virenprüfung erforderlich.
- Betriebssystem: Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2008 R2.
- Proxy-Server: Microsoft Forefront TMG 2010.

Nützliche Links

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

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

Vorteile

- Dr.Web für Qbik WinGate verfügt nicht nur über die entsprechende Dokumentation, sondern bietet zusätzlich technischen Support durch den Hersteller.
- Im Unterschied zu Konkurrenzprogrammen verfügt Doctor Web 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.

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.

Nützliche Links

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

Dr.Web für MIMEsweeper

Dr.Web für MIMEsweeper wird auf dem Computer mit MIMEsweeper installiert und führt die erste durch ClearSwift empfohlene Filterung durch

Vorteile

- Einfache Installation und Einstellung

  Die in Dr.Web für MIMEsweeper integrierten Konfigurationswerkzeuge 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-Header und E-Mail-Inhalt vom Content-Filter eingefügt werden.
- Flexible Einstellungen

  Bei der Detektion eines infektiösen 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-Inhalt 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, je nach 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 deshalb 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 von White- und Blacklists).
- Sammlung von Statistiken.
- Automatisches Update.

Systemanfoderungen

- HDD: 60 MB.
- Windows 2000 Server mit SP4 oder höher und Windows Server 2003/2008/2008 R2.
- E-Mail-Filter ClearSwift MIMEsweeper™ für SMTP 5.2 oder höher.

Nützliche Links

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

Dr.Web Mobile Security Suite

Schutz für mobile Endgeräte

- Dr.Web für Android
- Dr.Web für BlackBerry

Lizenzierung

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

Lizenzvarianten

Dr.Web für Android	Dr.Web für BlackBerry
■ Rundumschutz + Verwaltungscenter	■ Rundumschutz

Dr.Web für Windows Mobile kann separat oder inklusive in Dr.Web Enterprise Security Suite erworben werden. Im zweiten Fall wird das Verwaltungscenter von Dr.Web Enterprise Security Suite zusätzlich lizenziert.

Die Produkte der Gruppe Dr.Web Mobile Security Suite sind ist auch im kostengünstigen Dr.Web Small Business Bundle verfügbar.

	Dr.Web für Android	Dr.Web für BlackBerry
Schutzkomponenten*	Antivirus Antispam** Diebstahlschutz** URL-Filter Firewall Sicherheits-Revisor	Antivirus Sicherheits-Revisor
Zentrale Verwaltung in Dr.Web Enterprise Security Suite	+	+
Unterstützte Betriebssysteme	Android OS 4.0–7.1 Die Firewall läuft unter Android Version 4.0 und Android TV 5.0+	BlackBerry Version 10.3.2+
Schlüsselfunktionen		
Mehrströmige Scans und Verteilung der Auslastung zwischen mehreren Prozessorkernen.	+	
Prüfung von Dateien, die via GPRS/Infrared/Bluetooth/Wi-Fi/USB bzw. während der Synchronisierung mit dem PC übertragen werden	+	+
Zwei Scan-Modi: vollständig und benutzerdefiniert	+	+
Aktivieren/Deaktivieren der permanenten Prüfung der Speicherkarte	+	
Automatische Wiederherstellung der Funktionsfähigkeit	+	
Prüfung des ganzen Dateisystems oder einzelner Dateien und Verzeichnisse auf Anforderung	+	+
Prüfung von Dateien in APK-, ZIP-, SIS-, CAB-, RAR-Archiven	+	+
Start-Sperre für Apps, die durch den Administrator nicht freigegeben wurden.	+	
Definierbare Regeln für jede App	+	
Kontrolle von ein- und ausgehenden Daten für jede App	+	
Einschränkung des mobilen Datenverbrauchs	+	
Definierbare Einschränkungen für Apps im Roaming	+	
Sperrung des Zugriffs auf unerwünschte Web-Inhalte	+	
Schutz vor unerlaubten Zugriffen beim Verbinden mit Wi-Fi-Netzwerken	+	
Neutralisierung von Encodern und Dekodierung von verschlüsselten Daten	+	
Prüfung auf Sicherheitslücken	+	
Black- und Whitelists eingehender Anrufe und Kurznachrichten	+	
Unterstützung mehrerer SIM-Karten	+	
Löschen infizierter Dateien	+	+
Verschieben verdächtiger Dateien in die Quarantäne	+	+
Wiederherstellen von Dateien aus der Quarantäne	+	+
Update per Internet: ■ Via HTTP über das integrierte GPRS-Modul; ■ Via Infrared/Bluetooth/Wi-Fi/USB; ■ Durch die Synchronisierung mit dem PC, der über eine Internetverbindung verfügt, via ActiveSync	+	+
Detaillierte Protokolle mit Ergebnissen der Prüfung	+	+
Benachrichtigung über gefundene Bedrohungen auf der Sperroberfläche, von der man zur Liste von Bedrohungen übergehen kann	+	
Benachrichtigung über Aktionen, die für böswillige Apps charakteristisch sind	+	
Remote-Verwaltung eines mobilen Endgeräts bei dessen Verlust oder Diebstahl durch Diebstahlschutz	+	
GPS-Koordinaten des mobilen Geräts in einer SMS erhalten	+	

* Für Geräte unter Android TV sind nur Antivirus, Sicherheits-Revisor und Firewall verfügbar.

** Diese Komponente kann auf Endgeräten ohne SIM-Karte nicht benutzt werden.

Sonderangebot

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

- Allen Dr.Web Box-Produkten
- Dr.Web Security Space
- Dr.Web Antivirus für Windows

Nützliche Links

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

Dr.Web Bundles

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

	Geschützte Objekte	Lizenz	Umfang
Dr.Web Desktop Security Suite	Workstations	Rundumschutz	5 – 50
Dr.Web Server Security Suite	Server	Antivirus	1
Dr.Web Mail Security Suite	E-Mail-Anwender	Antivirus + Antispam	Entspricht der Anzahl an Workstations
Dr.Web Gateway Security Suite	Anwender von E-Mail- und Internet-Gateways	Antivirus	Entspricht der Anzahl an Workstations (ab 25)
Dr.Web Mobile Security Suite	Mobile Endgeräte	Antivirus + Antispam	Entspricht der Anzahl an Workstations

Dr.Web Universal Bundle

Kostengünstiger Rundumschutz der Enterprise-Klasse für kleine und mittelständische Unternehmen.

Kleine Unternehmen verfügen häufig über keine großen Budgets für den Rundumschutz. Für diese Unternehmen (mit 5-100 PCs) ist Dr.Web Universal Bundle gedacht.

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

Nützliche Links

Produktbeschreibung:
http://products.drweb-av.de/bundles/universal/

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 Windows-Servern, wenn die Antivirensoftware eines anderen Herstellers versagt. ■ Qualitätstest für das Antivirenprogramm eines anderen Herstellers.
Besonderheiten	■ Deinstallation des Antivirenprogramms eines anderen Herstellers vor der Prüfiung 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://www.drweb-curenet.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) , iPhone 4, iPod touch 4 iOS 7.0+.
Was ist "Mein Dr.Web CureNet!"?	„Mein Dr.Web CureNet!" 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.
Demoversion	Ohne Desinfektions-Funktion.

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 Windows-Servern, wenn die Antivirensoftware eines anderen Herstellers versagt. ■ Qualitätstest für das Antivirenprogramm eines anderen Herstellers.
Besonderheiten	■ Dr.Web CureIt! erfordert keine Installation und ist mit beliebigen Antivirusprogrammen kompatibel. Das installierte Antivirusprogramm eines anderen Herstellers muss dabei nicht ausgeschaltet werden. ■ Dr.Web CureIt! verfügt über einen hervorragenden Selbstschutz und kann Windows-Blockern effizient Widerstand leisten. ■ Dr.Web CureIt! wird mehrmals pro Stunde aktualisiert. ■ Das Tool kann von einem beliebigen externen Datenträger (u.a. USB-Speicher) gestartet werden.
Produktbeschreibung	http://www.freedrweb.com/cureit/
Unterstützte Betriebssysteme	MS Windows XP/Vista/7/8/8.1/10/ 2003/2008/2012 (32 und 64 Bit). HDD: Mindestens 100 MB.
Lizenzierung	Die Lizenzierung richtet sich nach der Anzahl an Workstations. Lizenzlaufzeit: 1 oder 10 Tage. Es sind auch Service-Lizenzen für 30 und 365 Tage vorgesehen. Mit diesen Lizenzen können Dienstleistungen in der Desinfektion von Unternehmensnetzwerken durch Dr.Web CureIt! Dritten angeboten werden.
Besonderheiten der Lizenzierung	Das Tool ist kostenlos für die Desinfektion Ihres eigenen Home-PCs.
Demoversion	Nicht vorhanden.

Russische Föderation

Doctor Web Ltd.

Tretja Uliza Jamskogo polja 2-12A, 125040 Moskau

Telefon: +7 (495) 789-45-87

Fax: +7 (495) 789-45-97

Internet: www.drweb.com | www.av-desk.com | www.free.drweb.com

Deutschland

Doctor Web Deutschland GmbH

Quettigstraße 12

76530 Baden-Baden

Telefon: +49 (0) 170 488 40 28

Internet: www.drweb-av.de

Republik Kazachstan

Doctor Web Zentralasien

Shevchenko 165B, Büro 910, 05009 Almaty

Telefon: +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 Technischer Support

Uliza Kostelnaja 4-3, 01001 Kiev

Telefon/Fax: +380 (44) 238-24-35, +380 (44) 279-77-70

E-Mail: dr.web@drweb.ua

Internet: www.drweb.ua

Frankreich

Doctor Web France

333 b Avenue de Colmar, 67100 Straßburg

Telefon: + 33 (0) 3-90-40-40-20

Fax : + 33 (0) 3-90-40-40-21

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

Telefon: +81 (0) 44-201-7711

Internet: www.drweb.co.jp

China

Doctor Web Software Company (Tianjin), Ltd.

Add: 112, North software tower, 80, 4th Avenue, TEDA, Tianjin, China

Director: Liu Dongsheng

Telefon: +86-022-59823480

E-mail: d.liu@drweb.com

© Doctor Web Ltd.,
2003–2020