



Proteggi ciò che hai creato

## Linea di prodotti Dr.Web Security Suite

### Guida delle licenze

Aggiornata il 10.06.2016

## Sommario

L'azienda Dr.Web .....	4
Tecnologie Dr.Web .....	4
Licenze e certificati di approvazione .....	9
Certificato di licenza Dr.Web .....	10
Linea di prodotti Dr.Web Security Suite .....	11
Licenze dei prodotti Dr.Web .....	11
Formati disponibili dei prodotti Dr.Web .....	13
Dr.Web Home Security Suite – prodotti per uso domestico .....	16
Prodotti .....	16
Dr.Web Security Space .....	17
Dr.Web Antivirus per Windows .....	21
Dr.Web Katana .....	23
Dr.Web Antivirus per OS X .....	24
Dr.Web Antivirus per Linux .....	24
Dr.Web Scanner a linea di comando .....	25
Dr.Web Mobile Security .....	26
Dr.Web per Android .....	26
Dr.Web per Blackberry .....	27
Dr.Web Enterprise Security Suite. Prodotti per l'impresa .....	28
Come scegliere il prodotto giusto: l'algoritmo .....	29
Pannello di controllo Dr.Web .....	30
Dr.Web Desktop Security Suite .....	32
Dr.Web Server Security Suite .....	33
Dr.Web per Windows Server .....	33
Dr.Web per OS X Server .....	35
Dr.Web per Novell NetWare Server .....	36
Dr.Web per UNIX Server .....	37
Dr.Web Mail Security Suite .....	38
Dr.Web per UNIX mail server .....	40
Dr.Web per MS Exchange .....	43
Dr.Web per IBM Lotus Domino .....	45
Dr.Web per Kerio mail server .....	46
Dr.Web Gateway Security Suite .....	47
Dr.Web per UNIX Internet Gateway .....	48

Dr.Web per Kerio Internet Gateway .....	49
Dr.Web per MIMESweeper .....	50
Dr.Web per Qbik WinGate .....	51
Dr.Web Mobile Security Suite .....	52
Dr.Web Retail Security Suite .....	54
Pacchetti Dr.Web .....	54
Utilità di disinfezione Dr.Web .....	55
Soluzioni .....	57
Web service .....	59
Politica di sconti .....	61
Condizioni generali di vendita .....	63
Acquisto supplementare in caso di Dr.Web Enterprise Security Suite .....	65
Codici dei prodotti, dei pacchetti, delle utilità e delle combinazioni di dispositivi e programmi Dr.Web .....	66
Contatti .....	69

## L'azienda Dr.Web

L'azienda Doctor Web S.r.l. è un produttore russo di mezzi di sicurezza informatica ben conosciuti nella Russia e in diversi paesi del mondo.

I prodotti antivirus Dr.Web esistono dal 1992 e ottengono da sempre i migliori risultati nel rilevamento e nell'eliminazione di software dannoso. La fondazione dell'azienda Doctor Web nel dicembre del 2003 ha spinto una crescita impetuosa della vendita dei prodotti Dr.Web sia nella Russia, sia in altri paesi.

Oggi Doctor Web è un'azienda che cresce velocemente e ottiene molti successi e che può essere considerata una presenza leader sul mercato di mezzi di sicurezza informatica. Noi disponiamo del nucleo antivirus di nostra produzione, abbiamo un nostro laboratorio per analizzare i codici dannosi, un servizio di monitoraggio antivirus globale e un servizio di supporto tecnico.

L'obiettivo strategico di Doctor Web al quale sono diretti gli sforzi del nostro team è la creazione dei mezzi di protezione antivirale che soddisfino tutte le esigenze di oggi. Ugualmente importante è lo sviluppo delle nuove soluzioni tecnologiche che consentono agli utenti di essere ben attrezzati per combattere qualsiasi minaccia proveniente da Internet. Essendo estremamente attuale, la linea dei prodotti Dr.Web abbraccia un'ampia gamma dei sistemi operativi e delle applicazioni compatibili.

L'azienda detiene una rete di distribuzione tramite partner, avendo rinunciato alla vendita diretta agli utenti finali.

Tra gli utenti dei nostri prodotti ci sono persone private dai diversi paesi del mondo, le maggiori aziende russe, piccole imprese, istituzioni ed enti pubblici, cui siamo grati per il loro appoggio e la loro dedizione a Dr.Web mostrati nel corso dei molti anni. I nostri certificati e premi conferitici dallo Stato provano l'avanzato grado di affidabilità di Dr.Web, un antivirus creato dall'ingegno dei programmatori russi.

## Tecnologie Dr.Web

L'antivirus Dr.Web è una famiglia di software sviluppata dall'ingegno dei programmatori russi sotto la guida di Igor Danilov.

Doctor Web S.r.l. è uno tra i pochi fornitori antivirus nel mondo che dispongono della propria tecnologia unica del rilevamento e dell'eliminazione di codici dannosi. Abbiamo un proprio servizio di monitoraggio antivirus e un laboratorio analitico e grazie a questo i nostri professionisti sono in grado di reagire velocemente alle nuove minacce e di aiutare i clienti a risolvere qualsiasi problema di qualunque complessità entro poche ore.

La caratteristica fondamentale di Dr.Web è la sua architettura modulare. Tutti i prodotti e le soluzioni Dr.Web contengono un nucleo antivirus comune e usano il sistema unificato degli aggiornamenti del database virus e il sistema globale del supporto tecnico. Le tecnologie Dr.Web rendono possibile organizzare una sicura difesa informatica sia nelle grandi reti aziendali, sia sul computer domestico oppure nell'ufficio di casa.

Oltre ai virus e i malware, Dr.Web è capace di rilevare e rimuovere dal computer diversi programmi indesiderati (quali adware, dialer, joke, le applicazioni potenzialmente pericolose, le applicazioni crack – spyware / riskware), lo spam e i messaggi elettronici indesiderati (i messaggi phishing, pharming, scamming e bounce).

### Tecnologie

Un programma antivirus di qualità deve sapere non solo come trovare i virus ma anche come pulirli. Una cosa è rimuovere i file infetti insieme alle informazioni preziose in essi contenute e un'altra cosa è ripristinarli allo stato originale pulito. Dr.Web tratta i file dell'utente con premura.

## Cura file dai virus

Un indicatore importante della qualità di un programma antivirale è la sua capacità di non soltanto trovare virus, ma di curare il computer dalle infezioni. Un buon antivirus non elimina file infetti insieme alle informazioni importanti contenute in essi, ma li ripristina allo stato originario pulito.

Prima di immettere in libera pratica virus tecnologicamente raffinati e molto pericolosi, creati a scopo di lucro, i loro autori li testano per accertarsi che essi non possano essere rilevati da nessun programma antivirale, affinché tali virus possano esistere più a lungo possibile senza essere scoperti. Prima dell'entrata dei campioni di tali virus nel laboratorio antivirale, essi non si rilevano da nessun antivirus.

## Dr.Web rileva virus con efficacia e cura infezioni sul computer

- Il software Dr.Web si distingue da tutti gli altri programmi analoghi perché può installarsi e funzionare sul computer già infetto e perché è molto resistente ai virus.
- Le tecnologie uniche di elaborazione dei processi in memoria e le capacità eccellenti di neutralizzazione delle infezioni attive consentono di installare Dr.Web immediatamente sulla macchina infetta (senza necessità di curarla prima) — è possibile avviare la scansione persino da un supporto rimovibile (quale chiave USB) senza installazione nel sistema e curare minacce attive già nel corso dell'installazione.
- L'integrazione del pacchetto di installazione Dr.Web (programma di installazione) con il componente aggiornato Dr.Web Antirootkit consente di combattere minacce attive e di curare il PC già nel corso dell'installazione dell'antivirus, se persino il computer sia infetto da programmi malevoli composti.
- Il sottosistema di scansione in background e di neutralizzazione delle minacce attive, realizzato nel componente Dr.Web Antirootkit (Antirootkit API, in forma abbreviata arkapi), risiede nella memoria e cerca minacce attive nelle aree critiche di Windows, quali oggetti in avvio automatico, processi e moduli in esecuzione, l'euristica per modifiche in oggetti di sistema, la memoria operativa, i MBR/VBR dei dischi, nonché il BIOS del computer. Rilevata una minaccia, il sottosistema cura l'infezione e blocca effetti dannosi.
- Dr.Web rileva e neutralizza i virus che risiedono nella memoria operativa e non si manifestano mai nella forma di un singolo file. **Finora, solo pochi programmi antivirali sono in grado di curare tali virus.**
- Dr.Web rileva con elevata esattezza oggetti malevoli pacchettati (anche se pacchettati da un metodo sconosciuto a Dr.Web), li scompone e li analizza dettagliatamente per scoprire minacce nascoste in essi.
- Solo Dr.Web è capace di controllare archivi per l'intero a qualsiasi livello di annidamento. Se persino un oggetto malevolo sia stato compresso più volte da programmi di compressione di diversi tipi, Dr.Web sicuramente rileva e neutralizza tale minaccia.

## Elevato livello di auto-protezione

Dr.Web è immune da ogni tentativo dei malware di metterlo fuori uso. La sua invulnerabilità è assicurata dal modulo di auto-protezione Dr.Web SelfPROtect che non ha pari sul mercato dei programmi antivirali.

- **Dr.Web SelfPROtect** è stato realizzato come driver e funziona al livello più profondo del sistema operativo. Il modulo non può essere scaricato o arrestato fino a quando il sistema non viene riavviato.
- **Dr.Web SelfPROtect** limita l'accesso dei malware alla rete, file e cartelle, alcuni rami del registro di sistema e supporti rimovibili agendo al livello di driver di sistema e protegge dai tentativi dei programmi anti-antivirus di arrestare Dr.Web.
- **Dr.Web SelfPROtect** è del tutto autosufficiente ed è diverso da alcuni prodotti concorrenti che modificano il nucleo di Windows (intercettano interrupt, sostituiscono tabelle di vettori, usano funzioni non documentate ecc.). Tali operazioni potrebbero provocare gravi problemi nel funzionamento del sistema operativo e creare nuovi modi per sfruttare vulnerabilità.
- Possibilità di ripristino automatico dei moduli.

## Tecnologie avanzate di protezione preventiva

- **FLY-CODE** è una tecnologia unica e universale di spaccettamento che consente di rilevare virus pacchettati, se persino pacchettati da programmi sconosciuti a Dr.Web.
- La tecnologia unica **Origins Tracing™** (una ricerca non basata sulle firme antivirali) consente a Dr.Web di rilevare con elevata probabilità le minacce che non sono ancora state inserite nella base di dati dei virus Dr.Web.
- L'analizzatore euristico Dr.Web rileva con efficacia le minacce di tutti i tipi più diffusi, determinando la loro categoria in base all'analisi e alle loro caratteristiche.
- A partire dalla versione 8.0, nei prodotti Dr.Web vengono utilizzate (e migliorate continuamente) le tecnologie di protezione preventiva del computer che includono la possibilità di bloccare modifiche automatiche degli oggetti critici di Windows e la possibilità di controllare alcune azioni non sicure.

## Tecnologie del filtro antispam

Le tecnologie della filtrazione Dr.Web Antispam consistono in svariate migliaia di regole le quali possono essere suddivise nei seguenti gruppi:

### ■ L'analisi euristica

Questa è una tecnologia eccezionalmente complessa che esegue l'analisi empirica di tutte le parti di un messaggio: l'oggetto, il corpo, ecc. Viene analizzato non solo il messaggio stesso ma anche l'eventuale allegato. L'analizzatore euristico si perfeziona di continuo e continuamente vengono aggiunte nuove regole. L'analizzatore euristico anticipa la comparsa delle nuove varietà di spam ancora sconosciute e consente d'identificarle prima che l'aggiornamento relativo sia rilasciato.

### ■ Filtrazione della resistenza spammer

La filtrazione della resistenza spammer è una delle tecnologie più avanzate ed efficaci del modulo antispam Dr.Web. Essa consiste nel riconoscimento dei trucchi usati dagli spammer per superare i filtri antispam.

### ■ L'analisi in base alle firme HTML

I messaggi che contengono il codice HTML vengono confrontati con il campionario delle firme HTML di antispam. Tale confronto in combinazione con i dati disponibili sulle misure delle immagini solitamente usate dagli spammer protegge gli utenti dai messaggi spam contenenti il codice HTML nei quali spesso vengono inserite delle immagini in linea.

### ■ Tecnologia del rilevamento dei procedimenti spammer applicati sulle buste dei messaggi

Il rilevamento dei falsi "timbri postali" di SMTP server e di altri falsi elementi contenuti negli oggetti dei messaggi email è la direzione più recente dello sviluppo dei metodi protettivi contro lo spam. Non si può affidarsi all'indirizzo del mittente di un messaggio elettronico perché può essere specificato un indirizzo falso. I messaggi falsificati non sono solo spam, essi possono essere raggiri o lettere anonime e persino minacciose usate per far pressione sugli utenti. Le tecnologie speciali di Dr.Web Antispam danno la possibilità di identificare gli indirizzi falsi e di non accettare tali messaggi. Questo consente di risparmiare traffico e di proteggere gli utenti dai messaggi falsi che li potrebbero spingere ad azioni imprevedibili.

### ■ L'analisi semantica

Durante quest'analisi le parole ed espressioni di un messaggio sono confrontate con le tipiche parole ed espressioni dello spam. Il confronto viene fatto in base al vocabolario apposito, e sono analizzate non solo le parole, le espressioni e i caratteri visibili ma anche quelli nascosti dall'occhio umano con diversi trucchi tecnici.

### ■ Tecnologia antiscamming

I messaggi scamming (nonché i messaggi pharming, un particolare tipo di scamming) sono forse la varietà più pericolosa dello spam. A essi appartengono: truffe alla nigeriana, notifiche di vincita al lotto o al casinò, false lettere di banche e di istituti di credito. Dr.Web Antispam applica un modulo speciale per filtrare tali messaggi.

## ■ Filtrazione dello spam tecnico

I messaggi bounce (ovvero i messaggi che tornano al mittente perché non recapitati) nascono come reazione ai virus oppure come una manifestazione dell'attività dei virus – per esempio a seguito dell'operazione di un worm postale che spedisce messaggi, o possono essere anche notifiche che un messaggio non è stato consegnato. Pertanto i messaggi bounce sono indesiderati nello stesso grado dello spam. Il modulo apposito di Dr.Web Antispam riconosce tali messaggi come messaggi indesiderati.

## Vantaggi di Dr.Web Antispam

- Verifica in tempo reale le email ricevute e inviate.
- Il funzionamento dell'antispam non dipende dal client di posta in uso e non aumenta il tempo della ricezione dei messaggi.
- L'antispam non deve essere configurato e comincia a operare automaticamente con la ricezione del primo messaggio.
- Le varie tecnologie di filtrazione assicurano un'alta probabilità dell'individuazione dello spam, dei messaggi phishing, pharming, scamming e bounce con una percentuale di errato riconoscimento vicina allo zero.
- I messaggi sottoposti al filtro non vengono eliminati ma spostati nell'apposita cartella del client di posta nella quale essi possono essere controllati in qualsiasi momento per accertarsi che non ci siano stati riconoscimenti sbagliati.
- Il modulo dell'analizzatore spam è assolutamente autonomo; per la sua operazione non occorre la connessione con un server esterno o l'accesso a qualunque database, il che consente di risparmiare notevolmente traffico.
- Gli aggiornamenti Dr.Web Antispam escono ogni giorno. Le tecnologie uniche dell'individuazione di messaggi indesiderati basate su migliaia di regole consentono di aggiornare il modulo non più spesso di una volta al giorno e pertanto di risparmiare traffico.

## L'organizzazione speciale del database virus di Dr.Web

La dimensione del database virus di Dr.Web è la più piccola tra tutti i programmi antivirus esistenti. Ciò è stato raggiunto grazie alla tecnologia propria della creazione del database virus in base al linguaggio molto flessibile elaborato specialmente per quanto riguarda la descrizione dei database. La dimensione piccola del database virus assicura risparmio di traffico, consente di occupare molto meno spazio sul disco e nella memoria operativa in confronto ai database virus degli altri produttori. Grazie alla piccola dimensione del database i componenti del programma Dr.Web possono interagire con grande velocità non imponendo un peso eccessivo sul processore.

Qual è la cosa più importante in un programma antivirus? Assicurare la protezione contro i codici dannosi. La protezione viene assicurata, tra le altre cose, dall'inserimento delle firme antivirali nel database, le quali consentono di rilevare i virus. Tuttavia il numero delle firme antivirali inserite nel database non ci dice niente su quanti virus può riconoscere in realtà un programma antivirus. Si capisce perché il database di Dr.Web ha meno firme antivirali dei database di alcuni altri produttori, quando si realizza che non tutti i virus sono esclusivi. Ci sono intere famiglie di virus affini (analoghi), ci sono perfino virus fatti da costruttori virus. Gli sviluppatori di alcuni altri antivirus registrano ogni virus affine come una firma antivirale separata, il che appesantisce il database. Un altro principio è stato applicato per il database virus di Dr.Web, dove una sola firma antivirale consente di rendere innocui decine o centinaia, talvolta persino migliaia di virus analoghi.

## Vantaggi del database virus di Dr.Web

- Il numero assolutamente minimale delle firme antivirali.
- Il piccolo volume degli aggiornamenti.
- Una sola firma consente di riconoscere decine o centinaia, talmente persino migliaia di virus analoghi.

La differenza principale che distingue il database virus di Dr.Web dai database di alcuni altri programmi antivirus è che avendo un numero minore delle firme antivirali esso consente di rivelare lo stesso (e persino un maggiore) numero di virus e di malware.

## **Che vantaggi danno all'utente la piccola dimensione del database virus di Dr.Web e il numero minimale delle firme antivirali?**

- Risparmio dello spazio sul disco.
- Risparmio delle risorse della memoria operativa.
- Risparmio del traffico nello scaricamento del database.
- Grande velocità dell'installazione del database e dell'elaborazione durante l'analisi dei virus.
- Capacità di riconoscere i virus che saranno creati nel futuro mediante la modificazione dei virus già esistenti.

## **Sistema globale degli aggiornamenti Dr.Web (Dr.Web GUS)**

- Il servizio del monitoraggio virus di Dr.Web raccoglie campioni di virus in tutto il mondo.
- Nuovi aggiornamenti escono immediatamente dopo che ogni nuova minaccia è stata analizzata e gli aggiornamenti sono stati predisposti.
- Prima di uscire, gli aggiornamenti vengono testati su una quantità immensa di file puliti.
- Gli aggiornamenti arrivano dagli utenti partendo da più server situati nei diversi punti del globo terrestre, il che minimizza il tempo necessario per riceverli.
- Il processo dell'aggiornamento dei database virus e dei moduli del software è completamente automatizzato.
- Gli aggiornamenti possono essere scaricati compressi in archivi.

## Licenze e certificati di approvazione

A differenza della maggioranza delle soluzioni concorrenti, i prodotti software Dr.Web Enterprise Security Suite versione 6 hanno i certificati di approvazione rilasciati dal Servizio Federale di Sicurezza e dal Servizio Federale di Controllo Tecnico e d'Esportazione della Russia. Questo consente di usarli negli enti che richiedono un elevato livello della sicurezza informatica.

Dr.Web è l'unico programma antivirus che ha ottenuto il certificato del Ministero della Difesa della Russia.

Dr.Web è completamente conforme alle prescrizioni della legge sulla protezione dei dati personali riguardanti prodotti antivirus, e può essere usato nelle reti che richiedono il massimo grado di protezione.

### L'azienda Dr.Web S.r.l. ha le seguenti licenze e certificati:

- le licenze del Servizio Federale di Controllo Tecnico e d'Esportazione della Russia per eseguire i lavori legati alla formazione dei mezzi di protezione dell'informazione, nonché per l'attività dello sviluppo e (o) produzione dei mezzi di protezione delle informazioni riservate;
- la licenza del Ministero della Difesa della Russia per l'attività della formazione dei mezzi di protezione delle informazioni;
- le licenze del Servizio Federale di Sicurezza della Russia per eseguire i lavori legati all'uso dei dati che costituiscono segreto di stato;
- la licenza del Centro di licenze, certificati e protezione di segreto di stato del Servizio Federale di Sicurezza per lo sviluppo e (o) produzione dei mezzi di protezione delle informazioni riservate;
- i certificati di approvazione del Servizio Federale di Sicurezza della Russia;
- i certificati di approvazione del Servizio Federale di Controllo Tecnico e d'Esportazione della Russia.



 **Tutte le licenze e i certificati di Dr.Web S.r.l. si trovano su:**

[http://company.drweb.com/licenses\\_and\\_certificates/](http://company.drweb.com/licenses_and_certificates/)

## Certificato di licenza Dr.Web

**ЛИЦЕНЗИОННЫЙ СЕРТИФИКАТ**  
**Dr.WEB®**

Настоящий сертификат удостоверяет, что данное программное обеспечение законно приобретено у разработчика и обладателя исключительных прав на антивирусное ПО семейства **Dr.WEB - ООО «Доктор Веб»**

Владелец лицензии	
Лицензируемый продукт	
Серийный номер	
Серийный номер	
Серийный номер	
Защищаемые объекты	
Рабочие станции	Серверы
Пользователи почты	Пользователи шлюза
Мобильные устройства	Центр управления
Срок лицензии	Поставщик

Генеральный директор  
ООО «Доктор Веб»  
Шаров В.А.

**Dr.Web Enterprise Security Suite**  
Комплексная защита всех узлов корпоративной сети  
**Dr.Web Enterprise Security Suite** – это комплекс продуктов Dr.Web, включающий элементы защиты всех узлов корпоративной сети и единый центр управления для безопасности из них.

<b>Dr.Web® Desktop Security Suite</b> Защита рабочих станций, клиентов терминальных и виртуальных серверов, клиентов встроенных систем	Windows, Linux, Mac OS X, MS DOS, OS2
<b>Dr.Web® Server Security Suite</b> Защита файловых серверов и серверов приложений (в том числе, терминальных и виртуальных серверов)	Windows, Novell NetWare, Novell Storage Services, Mac OS X Server, Unix
<b>Dr.Web® Mail Security Suite</b> Защита почты	Unix, MS Exchange, Lotus, Kerio
<b>Dr.Web® Gateway Security Suite</b> Защита шлюзов	Unix, Kerio, MMEsweepet, Qbik
<b>Dr.Web® Mobile Security Suite</b> Защита мобильных устройств	Android, Symbian OS, Windows Mobile

**Бонусы**  
При покупке **Dr.Web Desktop Security Suite** предоставляется право бесплатного использования:

- Dr.Web Mobile Security Suite
- Dr.Web CureIt!
- Dr.Web CureNet!

Il certificato di licenza Dr.Web è l'evidenza documentaria dell'uso legittimo del software Dr.Web da presentare alle autorità di vigilanza.

**IMPORTANTE! Il certificato di licenza Dr.Web non è il titolo per il rinnovo di una licenza o per la ricezione di uno sconto sul rinnovo.**

Il certificato di licenza ha un grado elevato di protezione. Non è possibile falsificarlo grazie al suo sfondo con disegno ornamentale particolare.

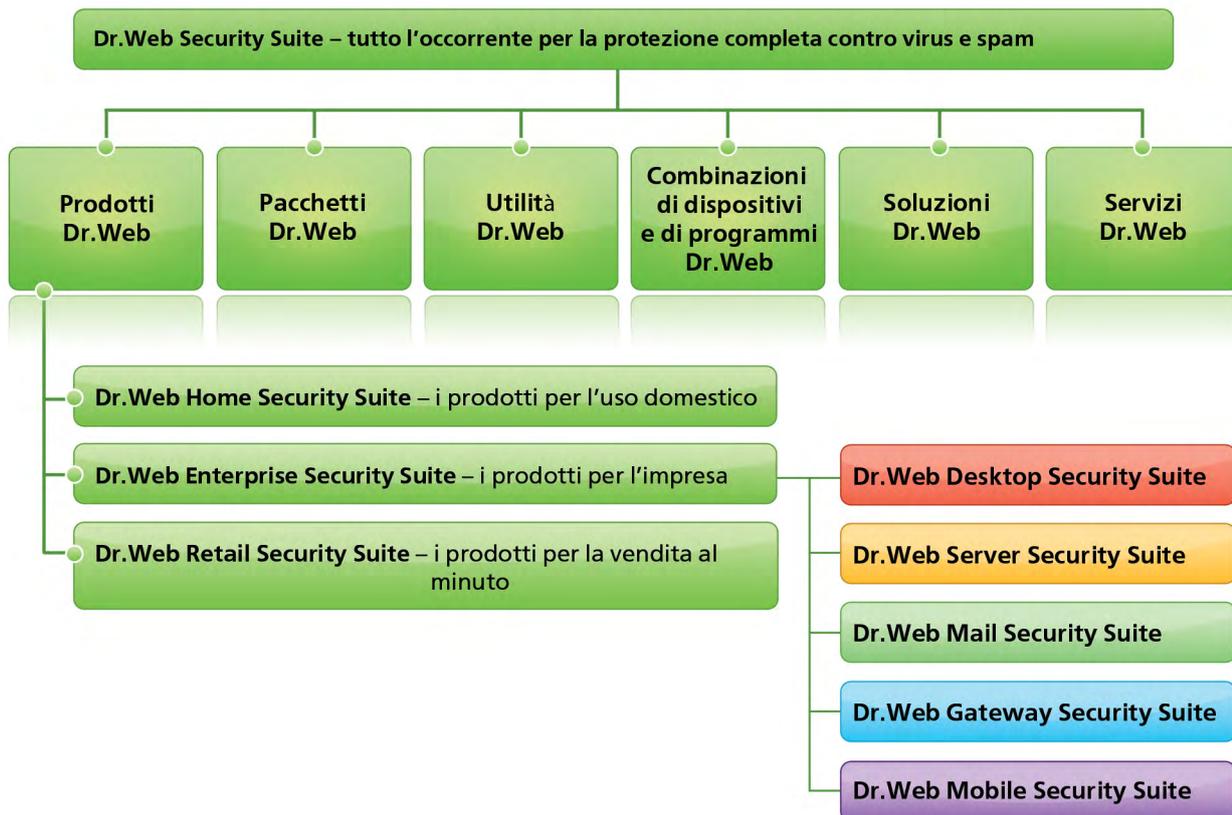
Il formulario del certificato di licenza è consegnato obbligatoriamente alle persone giuridiche con tutti i prodotti Dr.Web per aziende ed enti pubblici.

La copia elettronica del certificato di licenza può essere generata sulla pagina <http://products.drweb.com/register/certificate/>.

<ul style="list-style-type: none"> <li>■ Dr.Web® CureIt!</li> <li>■ Dr.Web® CureNet!</li> <li>■ Dr.Web® CureMail!</li> </ul> <p>Цены указаны с учетом доставки товара и доставки товара в адрес заказчика.</p>	<p>Минимум 1000 руб.</p>
<p>Защита программного обеспечения Dr.Web® Enterprise Security Suite</p>	<p>Минимум 1000 руб.</p>
<p>Защита почты Dr.Web® Mail Security Suite</p>	<p>Минимум 1000 руб.</p>
<p>Защита мобильных устройств Dr.Web® Mobile Security Suite</p>	<p>Минимум 1000 руб.</p>

## Linea di prodotti Dr.Web Security Suite

La linea di prodotti Dr.Web Security Suite comprende i prodotti commerciali per uso domestico, per l'impresa e per la vendita al minuto, i pacchetti, le utilità, le combinazioni di dispositivi e di programmi, le soluzioni e i servizi.



## Licenze dei prodotti Dr.Web

1. Le licenze dei prodotti Dr.Web hanno la durata di 12, 24 o 36 mesi. Le licenze dei prodotti Dr.Web Security Space e Dr.Web Antivirus per Windows sono anche disponibili con durata di 3 e 6 mesi.
2. Le licenze dei prodotti Dr.Web si acquistano secondo il tipo di oggetti da proteggere.
3. Gli oggetti da proteggere comprendono:
  - Workstation, client di terminal server e client di sistemi incorporati;
  - File server e server di applicazioni (compresi terminal server);
  - Utenti di posta elettronica;
  - Utenti di gateway mail e di gateway Internet;
  - Dispositivi mobili.

4. Sono previsti due tipi di **licenze di base**:
  - 1) Antivirus;
  - 2) Protezione Integrata.
5. La licenza di base **Protezione Integrata** è progettata solo per i prodotti che proteggono le workstation Windows.
6. La licenza della **Protezione Integrata** è composta di antivirus, antispam, antivirus per l'accesso web, parental control, firewall.
7. Gli elementi complementari della protezione richiesti dall'acquirente vengono aggiunti alla licenza di base. Non si può vendere una licenza per uno o più elementi complementari senza la vendita della licenza di base.
8. Per ogni tipo di oggetto da proteggere sono disponibili le apposite licenze di base e i propri set di elementi complementari.

Oggetti da proteggere	Sistemi operativi e piattaforme supportati	Licenza di base	Elementi complementari
<b>Dr.Web Desktop Security Suite</b> Workstation Client dei terminal server Client dei server virtuali Client dei sistemi incorporati	Windows 8.1 /8/7/ Vista/XP	Protezione integrata	■ Pannello di controllo
	OS X Linux	Antivirus	■ Pannello di controllo
	MS DOS* OS/2*		
<b>Dr.Web Server Security Suite</b> File server Server di applicazioni Terminal server Server virtuali	Windows Novell NetWare OS X Server UNIX (Samba)	Antivirus	■ Pannello di controllo
<b>Dr.Web Mail Security Suite</b> Utenti di posta elettronica	UNIX MS Exchange	Antivirus	■ Pannello di controllo ■ Antispam ■ SMTP proxy
	Lotus (Windows/Linux)		■ Antispam ■ SMTP prox
	Kerio (Windows/Linux)		■ SMTP prox
<b>Dr.Web Gateway Security Suite</b> Utenti di gateway Internet	Kerio Internet Gateway UNIX Internet Gateway	Antivirus	■ Pannello di controllo
	MIMESweeper* Qbik WinGate*		■ Antispam
<b>Dr.Web Mobile Security Suite</b> Dispositivi mobili	Windows Mobile Android	Protezione integrata	■ Pannello di controllo ■ Antispam
	Symbian OS*	Antivirus	■ Antispam
	Windows Mobile		

\* Il controllo centralizzato non è ancora disponibile.

## Formati disponibili dei prodotti Dr.Web

I programmi Dr.Web sono disponibili sotto forma di licenze elettroniche o di pacchetti media confezionati.

### 1. Licenze elettroniche Dr.Web

Sono assegnate per mezzo del numero seriale Dr.Web:

- spedito via posta elettronica;
- indicato sul certificato di licenza.

### 2. Pacchetti media Dr.Web nelle confezioni di cartone



#### Allestimento:

- Confezione di cartone commerciale Dr.Web
- Certificato di licenza
- Guida breve d'installazione e di registrazione
- Disco CD/DVD
- Busta commerciale Dr.Web per il disco
- Sigillo adesivo
- Adesivo con l'iscrizione «Protetto da Dr.Web»
- Chiavetta USB (solo per il prodotto Dr.Web per OS X + Dr.Web Security Space Pro).

### 3. Soluzione Dr.Web confezionata

Soluzione formata da uno o più prodotti Dr.Web Enterprise Security Suite.



#### Allestimento:

- Confezione di cartone commerciale Dr.Web;
- Formulario di certificato di licenza;
- Disco DVD con i file d'installazione del software Dr.Web nella busta commerciale Dr.Web.

## 4. Pacchetti media Dr.Web certificati

Soluzione formata da uno o più prodotti Dr.Web Enterprise Security Suite che sono stati certificati dal Servizio Federale di Controllo Tecnico e d'Esportazione della Russia.



### Allestimento:

- Confezione di cartone commerciale Dr.Web;
- Formulário di certificato di licenza;
- Disco DVD con i file d'installazione dei software Dr.Web certificati nella busta commerciale Dr.Web
- Formulário con l'adesivo olografico del Servizio Federale di Controllo Tecnico e d'Esportazione della Russia.

## 5. Licenza Dr.Web in busta di cartone

Soluzione formata da uno o più prodotti Dr.Web Enterprise Security Suite.



### Allestimento:

- Busta di cartone commerciale Dr.Web;
- Formulário di certificato di licenza.

## 6. Scheda da grattare

Scheda con il numero seriale Dr.Web coperto da una striscia da grattare.



## 7. Consegna di licenza OEM Dr.Web Prodotti OEM di Dr.Web

### Una scheda OEM con una striscia da grattare

Dr.Web Security Space

1 PC/3 mesi



#### Prima variante di consegna

- Scheda OEM con una striscia da grattare.

#### Seconda variante di consegna

- Scheda OEM con una striscia da grattare attaccata sul volantino OEM;
- Busta commerciale Dr.Web per il volantino OEM.

Se è stato accordato, è possibile fare schede OEM con il logotipo del partner.

# Dr.Web Home Security Suite – prodotti per uso domestico

## Prodotti

Dr.Web Security Space	Dr.Web Mobile Security
Protezione di qualunque dispositivo	Protezione dei dispositivi mobili
Programmi Dr.Web	
<ul style="list-style-type: none"> <li>■ Dr.Web Security Space</li> <li>■ Dr.Web Antivirus per Windows</li> <li>■ Dr.Web Antivirus per OS X</li> <li>■ Dr.Web Antivirus per Linux</li> </ul>	–
<ul style="list-style-type: none"> <li>■ Dr.Web per Android</li> <li>■ Dr.Web per Symbian</li> <li>■ Dr.Web per Windows Mobile</li> </ul>	<ul style="list-style-type: none"> <li>■ Dr.Web per Android</li> <li>■ Dr.Web per Symbian</li> <li>■ Dr.Web per Windows Mobile</li> </ul>

## Componenti di protezione in Dr.Web Security Space

Componenti di protezione	Windows	OS X	Linux
Antivirus	+	+	+
Antispam	+		
Monitoraggio HTTP	+		
Parental control	+		
Firewall	+		
Rete antivirale	+		

## Licenze di Dr.Web Security Space

1. Le licenze del prodotto vengono concesse sulla base del numero di computer protetti (1 – 5).
2. La variante della licenza è Protezione Completa.
3. Le durate delle licenze commerciali sono 3, 6, 12, 24 o 36 mesi. Le durate delle licenze OEM sono 3 o 6 mesi.
4. Si applicano gli sconti regolari sul rinnovo.
5. Non sono previsti alcuni altri sconti.
6. Gli acquirenti del prodotto hanno il diritto di usare gratuitamente Dr.Web Mobile Security. Il numero di dispositivi mobili protetti è uguale al numero di PC protetti.

## Ampliamento della licenza (acquisto supplementare)

1. In caso di Dr.Web Security Space, l'ampliamento della licenza consiste in: a) migrazione da Dr.Web Antivirus verso Dr.Web Security Space o b) aumento del numero di oggetti protetti.
2. La licenza di acquisto supplementare si attiva automaticamente al momento di generazione utilizzando le informazioni di registrazione della licenza precedente.
3. Se fino alla scadenza della licenza rimangono più di 3 mesi, il prezzo dell'ampliamento è il prezzo della licenza di rinnovo. Nel codice di tale licenza, il tipo di licenza è D. La licenza si rinnova automaticamente.

4. Se fino alla scadenza della licenza rimangono meno di 3 mesi,
  - la licenza viene ampliata gratuitamente tramite il [servizio di ampliamento gratuito](#);
  - la licenza precedente viene bloccata un giorno dopo la generazione di quella nuova;
  - nel codice della licenza nuova, il tipo di licenza è C, mentre il prezzo di tale licenza è pari allo zero. Il cliente potrà rinnovare successivamente questa licenza con lo sconto sul rinnovo.

## ► Dr.Web Security Space

Protezione completa per Windows, antivirus per OS X e Linux

- Una soluzione completa per la protezione dei computer Windows.
- Difesa in tempo reale.
- Il software può essere installato e funziona su un computer già infetto; è molto resistente ai malware.
- Rileva in modo efficiente qualsiasi tipo di minaccia informatica e ripulisce il sistema da qualsiasi virus.
- Alta velocità di scansione grazie all'utilizzo delle possibilità dei sistemi multiprocessore.
- Protegge dai malware più recenti che sono in grado di aggirare i metodi tradizionali dell'analisi basata sulle firme antivirali e dell'analisi euristica.
- Protezione dei dati contro eventuali danneggiamenti.
- Analisi integrata delle minacce pacchettate.
- Scansione completa degli archivi situati su qualsiasi livello di nidificazione.
- Migliore rilevamento e neutralizzazione dei virus compositi.
- Filtraggio dello spam e di tutti i tipi di email indesiderate senza necessità di istruire l'antispam.
- Scansione completa «a volo» di tutti i dati trasmessi su tutte le porte.
- Navigazione sicura in Google, Yandex, Yahoo!, Bing, Rambler grazie all'attivazione della funzione «Safe search» nei motori di ricerca – i contenuti non sicuri vengono filtrati direttamente dai motori di ricerca!
- Comunicazione sicura – filtraggio dei dati in messaggi istantanei.
- Protezione valida dei minori da contenuti indesiderati.
- Blocco della possibilità di utilizzare dispositivi rimovibili e il computer senza permesso.
- Servizio **Dr.Web Cloud** – controllo di URL sui server della società Doctor Web.
- Protezione da accessi da fuori non autorizzati, prevenzione di furti di informazioni, blocco di connessioni non attendibili a livello di pacchetti e applicazioni.
- Possibilità di gestire Dr.Web su remoto su altri computer in una rete locale senza dover installare il Pannello di controllo Dr.Web.

## Componenti di protezione

### Rilevamento efficace e pulizia del sistema dalle minacce di tutti i tipi (Scanner Dr.Web)

- Il controllo multithread in sistemi a più processori assicura l'alta velocità di scansione.
- Scansione molto accurata della memoria operativa, settori di avvio, dischi rigidi e supporti rimovibili alla ricerca di virus, cavalli di troia e altri tipi di oggetti malevoli.
- Rileva solo le minacce informatiche che sono capaci di funzionare.
- Ampi database per individuare spyware, riskware, adware, hacktool e joke.
- L'antirookit **Dr.Web Shield™**, incluso nello Scanner, individua virus compositi che utilizzano tecnologie rootkit e possono nascondere la loro presenza nel sistema infetto.

- Lo scanner console, uno dei componenti di Dr.Web, è progettato per gli utenti più esperti e consente di eseguire la scansione dalla linea di comando. Ha maggiori possibilità di configurazione e può essere usato anche in sistemi multiprocessore.

### Difesa in tempo reale (file monitor SpIDer Guard®)

- **Miglioramento!** Migliorate le prestazioni sulle macchine con un trasferimento di file intenso (un uso intenso di file system, per esempio, download di file da tracker dei torrent e di condivisione, compilazione e rendering) – grazie all’aggiornato sottosistema di scansione del componente Dr.Web SpIDer Guard.
- **SpIDer Guard** esegue un monitoraggio continuo della salute del computer intercettando “al volo” accessi ai file locati sui dischi, dischetti, CD/DVD/Blu-ray e schede di memoria.
- **SpIDer Guard** è molto resistente ai tentativi dei programmi malevoli di compromettere o interrompere il suo funzionamento.
- Le tecnologie del nucleo antivirale di Dr.Web controllano in maniera dinamica la disponibilità delle risorse del computer e contengono il loro consumo da parte dell’antivirus senza ridurre l’efficacia della protezione.

### Posta elettronica senza virus, spam e messaggi indesiderati

- Trasferimento delle email sicuro – si controllano su tutte le porte tutti i dati trasmessi attraverso i protocolli supportati da Dr.Web, compresi i protocolli protetti (se l’utente ha attivato il controllo SSL).
- Scansione delle email trasmesse attraverso i protocolli SMTP/POP3/NNTP/IMAP4 alla ricerca di virus e spam in tempo reale.
- Controllo delle connessioni cifrate SSL (SMTPS/POP3S/IMAP4S).
- La scansione non influisce sul funzionamento del client di posta in uso e non aumenta quasi per niente il tempo di ricezione delle email.
- Si applicano regole individuali di elaborazione per ciascun tipo di malware – virus, riskware, adware, hacktool, paid dialer e joke.
- Protezione contro i mailing in grandi quantità eseguiti da worm postali – la protezione è basata sull’analisi della struttura e del tempo di invio delle email in uscita perché questi indicatori possono evidenziare l’attività virale.

### Antispam

- L’antispam non richiede di essere configurato e comincia a funzionare automaticamente con la ricezione della prima email.
- Diverse tecnologie di filtraggio forniscono un’elevata probabilità di rilevamento dello spam e dei messaggi phishing, pharming, scamming e bounce.
- Protezione dal coinvolgimento nelle botnet – il provider non scollegherà il computer da Internet a causa della spedizione dello spam.
- Le email filtrate non vengono eliminate, ma spostate in una cartella speciale del client di posta, dove esse possono essere controllate in qualsiasi tempo per accertarsi che non vi siano stati falsi positivi.
- Il modulo analizzatore di spam è completamente autonomo; per il suo funzionamento non è necessaria una connessione a un server esterno o l’accesso a un database, quindi si risparmia il traffico.

### Scudo contro le minacce di Internet (Monitoraggio HTTP SpIDer Gate™)

- Il modulo **SpIDer Gate** scansiona in tempo reale e in modo trasparente il traffico HTTP in entrata, intercetta tutte le connessioni HTTP, filtra dati, blocca pagine infette automaticamente in qualunque browser, controlla file compressi in archivi (per esempio, file scaricati tramite download manager e molte altre applicazioni che scambiano dati con web server), protegge da siti phishing e da altri siti pericolosi.

- Trasferimento dei dati di Internet sicuro – si controllano su tutte le porte tutti i dati trasmessi attraverso i protocolli supportati da Dr.Web, compresi i protocolli protetti (se l'utente ha attivato il controllo SSL).
- Navigazione sul web sicura – con la funzione «Safe search» attivata, i motori di ricerca Google, Yandex, Yahoo!, Bing, Rambler visualizzano solo siti ritenuti sicuri dal punto di vista del motore di ricerca e di Dr.Web. Siti inaffidabili vengono esclusi dai risultati di una ricerca!
- Comunicazione sicura – si filtrano i dati trasferiti dai programmi di messaggistica istantanea Mail, Ru Agent, ICQ, Jabber. I link che conducono su siti malevoli o fraudolenti vengono cancellati dai messaggi. Si esegue un controllo antivirale degli allegati ai messaggi, e se un file è potenzialmente pericoloso, la sua spedizione viene impedita.
- Controlla le connessioni cifrate SSL (HTTPS).
- Impedisce l'accesso a siti web utilizzando il database dei virus conosciuti e dei siti non raccomandati per essere visitati. Un database speciale dei siti che divulgano contenuti senza consenso degli autori – protezione dei titolari dei diritti d'autore.
- È possibile disattivare il controllo del traffico in uscita o in entrata, nonché si può creare una lista delle applicazioni, il cui traffico HTTP verrà controllato in ogni caso e per l'intero (black list). Inoltre è possibile escludere dal controllo il traffico di alcune applicazioni (white list).
- È possibile impostare la priorità di scansione del traffico (rapporto di scansione). Il rapporto di scansione influisce sulla distribuzione delle risorse del processore e sulla velocità del lavoro in Internet.
- Il funzionamento di **SplDer Gate** non dipende dal browser in uso.
- Il filtraggio HTTP non ha quasi nessun effetto sulle prestazioni del computer, sulla velocità del lavoro in Internet e sulla quantità di dati trasmessi.
- Non è necessario configurare il modulo perché con le impostazioni predefinite **SplDer Gate** inizia la scansione subito dopo essere stato installato nel sistema.
- Controllo di URL sui server di Doctor Web tramite il servizio Dr.Web Cloud. Al tentativo di aprire un sito, questo servizio manda l'URL sui server di Doctor Web per controllo. Il controllo si esegue in tempo reale e non dipende dallo stato dei database virali Dr.Web sul computer dell'utente, né dalle impostazioni locali dell'aggiornamento.

## Controllo della navigazione in Internet e blocco dei supporti rimovibili (Controllo Genitori di Dr.Web)

- Trasferimento dei dati di Internet sicuro – si controllano tutti i dati trasmessi su tutte le porte.
- Protezione dei minori contro le visite sui siti web indesiderati.
- Possibilità di limitare il tempo di lavoro dell'utente sul web e al computer.
- È possibile impedire la modificazione dell'ora e del fuso orario di sistema – i figli non potranno utilizzare il computer nelle ore non permesse dai genitori.
- Profili individuali del Controllo Genitori possono essere configurati separatamente per ciascun utente.
- Possibilità di limitare l'accesso a periferiche quali unità disco, unità DVD/CD-ROM, la tastiera, il mouse, schede di rete, lettori audio e video, periferiche di gioco, dispositivi USB, porte COM/LPT.
- Le white list dei dispositivi affidabili impediscono che un dispositivo rimovibile venga connesso in maniera non autorizzata al computer protetto da Dr.Web, difendono dati confidenziali contro furti attraverso una chiavetta USB e non lasciano che virus penetrino nel sistema attraverso dispositivi USB che oggi sono una fonte di malware più comune. Esportazione/importazione delle white list.
- Impedisce l'accesso a siti web basandosi su dieci gruppi tematici (armi, droga, giochi, pornografia ecc.).
- Proibisce di usare supporti rimovibili (quali unità di memoria flash, dispositivi USB), dispositivi di rete e singoli file e cartelle fornendo una possibilità aggiuntiva di proteggere i dati personali e le informazioni importanti contro rimozione o furto da parte dei malintenzionati.
- Controllo in tempo reale di URL sui server di Doctor Web tramite il servizio Dr.Web Cloud – l'efficienza di rilevamento non dipende dallo stato dei database virali Dr.Web sul computer dell'utente, né dalle impostazioni locali dell'aggiornamento.

- Si può impedire l'invio dei task alla stampante – protegge da una stampatura non autorizzata di documenti confidenziali e permette di risparmiare carta.

### Protezione contro gli attacchi sulla rete (Firewall Dr.Web)

- Protezione contro l'accesso non autorizzato tentato dall'esterno; prevenzione di fughe dei dati importanti attraverso la rete; arresto delle connessioni inattendibili a livello di pacchetti e applicazioni.
- Nuovo tipo di database del firewall Dr.Web – rende più conveniente la creazione delle regole da parte dell'utente. Adesso il firewall Dr.Web utilizza un database delle applicazioni affidabili. L'affidabilità delle applicazioni si basa sul certificato digitale. Tutti i programmi legittimi dal punto di vista di Dr.Web possono connettersi a qualsiasi URL su qualsiasi porta. Eccezione: se un programma non ha una firma digitale valida o non ne ha nessuna (per esempio, freeware oppure open source), il firewall chiede all'utente di creare una regola opportuna.
- Il filtraggio fatto a livello di applicazioni consente di controllare tentativi di accesso dei singoli programmi e processi a siti web e di registrare tali tentativi di accesso nel log delle applicazioni.
- Il filtraggio fatto a livello di pacchetti consente di controllare l'accesso a Internet indipendentemente dai programmi che avviano la connessione. Il log del filtro pacchetti conserva informazioni sui pacchetti trasmessi attraverso le interfacce di rete.
- Se è abilitata la cosiddetta "modalità di gioco", le richieste del Firewall di creare una regola di accesso compaiono sopra qualsiasi applicazione avviata a schermo intero.
- Monitoraggio delle applicazioni che usano la rete in tempo reale con la possibilità di chiudere forzatamente una connessione.

### Amministrazione remota

- Tramite il componente Rete antivirus è possibile amministrare e configurare su remoto gli antivirus Dr.Web installati sui computer di una rete locale.
- Per amministrare gli antivirus su remoto, non è necessaria l'installazione del Pannello di Controllo Dr.Web.
- La connessione è possibile da qualsiasi computer a qualsiasi altro computer all'interno della rete locale.
- Amministrando gli antivirus su remoto, si possono ricevere statistiche e log dalla postazione remota, leggere e modificare impostazioni dei moduli sulla postazione remota, avviare e fermare tali moduli. Inoltre sulla postazione remota si può registrare il numero di serie e cambiare il file della chiave.
- Per accedere su remoto a una postazione, è necessario consentire l'accesso remoto su questa postazione.

### Requisiti di sistema

#### Per Dr.Web Security Space

- Windows 8/7/Vista (declinazioni a 64 bit) e Windows 8/7/Vista/XP SP2 (declinazioni a 32 bit). Spazio disponibile sul disco rigido: ~550 MB. File temporanei generati durante l'installazione richiedono uno spazio aggiuntivo. Per installare il firewall sono necessari altri ~ 7 MB.

**Requisiti aggiuntivi:** l'accesso a Internet per registrarsi e ricevere aggiornamenti.

### Licenze

#### Tipi di licenze

- Secondo il numero di workstation protette.

#### Varianti di licenze

- Protezione completa

### Link utili

Descrizione: [http://products.drweb.com/win/security\\_space](http://products.drweb.com/win/security_space)

## ► Dr.Web Antivirus per Windows

Protezione minima da programmi malevoli per Windows, OS X, Linux

- Una soluzione completa per la protezione dei computer Windows.
- Difesa in tempo reale.
- Il software può essere installato e funziona su un computer già infetto; è molto resistente ai malware.
- Rileva in modo efficiente qualsiasi tipo di minaccia informatica e ripulisce il sistema da qualsiasi virus.
- Alta velocità di scansione grazie all'utilizzo delle possibilità dei sistemi multiprocessore.
- Protegge dai malware più recenti che sono in grado di aggirare i metodi tradizionali dell'analisi basata sulle firme antivirali e dell'analisi euristica.
- Protezione dei dati contro eventuali danneggiamenti.
- Analisi integrata delle minacce pacchettate.
- Scansione completa degli archivi situati su qualsiasi livello di nidificazione.
- Migliore rilevamento e neutralizzazione dei virus compositi.
- Filtraggio dello spam e di tutti i tipi di email indesiderate senza necessità di istruire l'antispam.
- Scansione completa «a volo» delle email su tutte le porte.
- Protezione da accessi da fuori non autorizzati, prevenzione di furti di informazioni, blocco di connessioni non attendibili a livello di pacchetti e applicazioni.

## Componenti di protezione

### Rilevamento efficace e pulizia del sistema dalle minacce di tutti i tipi (Scanner Dr.Web)

- Il controllo multithread in sistemi a più processori assicura l'alta velocità di scansione.
- Scansione molto accurata della memoria operativa, settori di avvio, dischi rigidi e supporti rimovibili alla ricerca di virus, cavalli di troia e altri tipi di oggetti malevoli.
- Rileva solo le minacce informatiche che sono capaci di funzionare.
- Ampi database per individuare spyware, riskware, adware, hacktool e joke.
- L'antirrootkit Dr.Web Shield™, incluso nello Scanner, individua virus compositi che utilizzano tecnologie rootkit e possono nascondere la loro presenza nel sistema infetto.
- Lo scanner console, uno dei componenti di Dr.Web, è progettato per gli utenti più esperti e consente di eseguire la scansione dalla linea di comando. Ha maggiori possibilità di configurazione e può essere usato anche in sistemi multiprocessore.

### Difesa in tempo reale (file monitor SpIDer Guard®)

- **Miglioramento!** Migliorate le prestazioni sulle macchine con un trasferimento di file intenso (un uso intenso di file system, per esempio, download di file da tracker dei torrent e di condivisione, compilazione e rendering) – grazie all'aggiornato sottosistema di scansione del componente Dr.Web SpIDer Guard.
- **SpIDer Guard** esegue un monitoraggio continuo della salute del computer intercettando "al volo" accessi ai file locati sui dischi, dischetti, CD/DVD/Blu-ray e schede di memoria.
- **SpIDer Guard** è molto resistente ai tentativi dei programmi malevoli di compromettere o interrompere il suo funzionamento.
- Le tecnologie del nucleo antivirale di Dr.Web controllano in maniera dinamica la disponibilità delle risorse del computer e contengono il loro consumo da parte dell'antivirus senza ridurre l'efficacia della protezione.

## Posta elettronica senza virus

- Trasferimento delle email sicuro – si controllano su tutte le porte tutti i dati trasmessi attraverso i protocolli supportati da Dr.Web, compresi i protocolli protetti (se l'utente ha attivato il controllo SSL).
- Scansione delle email trasmesse attraverso i protocolli SMTP/POP3/NNTP/IMAP4 alla ricerca di virus in tempo reale.
- Controllo delle connessioni cifrate SSL (SMTPS/POP3S/IMAP4S).
- La scansione non influisce sul funzionamento del client di posta in uso e non aumenta quasi per niente il tempo di ricezione delle email.
- Si applicano regole individuali di elaborazione per ciascun tipo di malware – virus, riskware, adware, hacktool, paid dialer e joke.
- Protezione contro i mailing in grandi quantità eseguiti da worm postali – la protezione è basata sull'analisi della struttura e del tempo di invio delle email in uscita perché questi indicatori possono evidenziare l'attività virale.

## Protezione contro gli attacchi sulla rete (Firewall Dr.Web)

- Protezione contro l'accesso non autorizzato tentato dall'esterno; prevenzione di fughe dei dati importanti attraverso la rete; arresto delle connessioni inattendibili a livello di pacchetti e applicazioni.
- Nuovo tipo di database del firewall Dr.Web – rende più conveniente la creazione delle regole da parte dell'utente. Adesso il firewall Dr.Web utilizza un database delle applicazioni affidabili. L'affidabilità delle applicazioni si basa sul certificato digitale. Tutti i programmi legittimi dal punto di vista di Dr.Web possono connettersi a qualsiasi URL su qualsiasi porta. Eccezione: se un programma non ha una firma digitale valida o non ne ha nessuna (per esempio, freeware oppure open source), il firewall chiede all'utente di creare una regola opportuna.
- Il filtraggio fatto a livello di applicazioni consente di controllare tentativi di accesso dei singoli programmi e processi a siti web e di registrare tali tentativi di accesso nel log delle applicazioni.
- Il filtraggio fatto a livello di pacchetti consente di controllare l'accesso a Internet indipendentemente dai programmi che avviano la connessione. Il log del filtro pacchetti conserva informazioni sui pacchetti trasmessi attraverso le interfacce di rete.
- Se è abilitata la cosiddetta "modalità di gioco", le richieste del Firewall di creare una regola di accesso compaiono sopra qualsiasi applicazione avviata a schermo intero.
- Monitoraggio delle applicazioni che usano la rete in tempo reale con la possibilità di chiudere forzatamente una connessione.

## Requisiti di sistema

- Intel® Pentium® IV con frequenza di 1,6 GHz.
- 512 MB di memoria operativa.
- File temporanei creati durante l'installazione richiedono spazio aggiuntivo.
- Almeno 330 MB di spazio su disco rigido
- Windows 2012/8/7/2008/Vista/2003/XP SP 2 (sistemi a 32 e 64 bit).
- OS X 10.7 o superiore (declinazioni a 32 e a 64 bit).
- Linux 2.6 o superiore (declinazioni a 32 e a 64 bit).

**Requisiti aggiuntivi:** l'accesso a Internet per registrarsi e ricevere aggiornamenti.

## Licenze

### Tipi di licenze

- Secondo il numero di workstation protette

### Varianti di licenze

- Antivirus (la licenza include i seguenti componenti di protezione: antivirus, antispyware, antiroot-kit, firewall)

## Link utili

Descrizione: <http://products.drweb.com/win/av/>

## ► Dr.Web Katana

Un antivirus non basato su firme che fornisce la protezione preventiva contro le minacce recenti sconosciute dall'antivirus in uso, contro gli attacchi mirati e i tentativi da parte dei trojan e degli exploit di sfruttare le vulnerabilità, incluse quelle zero-day, per penetrare nei sistemi.

### Vantaggi

- Neutralizza i programmi malevoli recenti non ancora conosciuti dall'antivirus in uso, capaci di aggirare il rilevamento fornito dalla scansione tradizionale basata su firme e dai metodi euristici.
- Inizia a proteggere il sistema nella fase di partenza del sistema operativo persino prima che venga caricato l'antivirus tradizionale basato su firme!
- Neutralizza le attività dei programmi malevoli attivi senza sovraccaricare il sistema.
- Analizza il comportamento di ogni minaccia in tempo reale confrontandolo con le informazioni sulla reputazione conservate in Dr.Web Cloud che vengono aggiornate di continuo. Neutralizza immediatamente gli script e i processi nocivi che l'antivirus in uso non ha potuto riconoscere. Monitora tutti i processi di sistema e blocca quelli che manifestano un comportamento malevolo. Determina se un programma è malevolo e quindi prende ogni provvedimento necessario per neutralizzare la minaccia.
- Non richiede alcuna configurazione e inizia a funzionare efficacemente subito dopo l'installazione.
- Protegge il sistema persino se il PC non è connesso a Internet.

### Funzioni

- Protegge le aree critiche del sistema dalle modifiche che i programmi malevoli possono apportare.
- Rileva e impedisce l'esecuzione degli script e dei processi malevoli, sospetti o inattendibili.
- Rileva le modifiche indesiderate dei file, monitora il funzionamento di tutti i processi per rilevare le azioni tipiche dei malware (per esempio le attività dei cryptolocker) e impedisce agli oggetti malevoli di iniettare il proprio codice in altri processi.
- Rileva e neutralizza le minacce che non sono ancora state scoperte e inserite nel database dei virus Dr.Web: per esempio nuovi programmi-estorsori cryptolocker, web injector.
- Protegge dagli exploit – oggetti malevoli che si approfittano delle falle nei software, comprese quelle che non sono ancora conosciute da nessuno tranne che dagli hacker che hanno creato l'exploit corrispondente (le vulnerabilità zero-day).
- Controlla il funzionamento dei browser più popolari e dei plugin associati; protegge dai programmi che bloccano i browser.
- Blocca la capacità dei malware di modificare le aree del disco di avvio per impedire l'avvio dei trojan, per esempio, sul computer.
- Protegge dalle modifiche il registro di Windows per assicurare che la modalità provvisoria non venga disabilitata.
- Non permette ai programmi malevoli di modificare le routine di base del sistema. Bloccando determinate chiavi del registro di Windows impedisce ai malware di modificare l'aspetto del desktop o di nascondere programmi trojan tramite un rootkit.
- Ostacola le modifiche dei permessi di avvio da parte dei malware.
- Non permette che i driver nuovi o sconosciuti vengano scaricati senza il consenso dell'utente.
- Impedisce ai programmi malevoli e a determinate applicazioni, quali gli anti-antivirus, di aggiungere record al registro di Windows per assicurare la propria esecuzione automatica.
- Chiude le sezioni del registro contenenti le informazioni sui driver di periferica virtuale assicurando che non vengano create nuove periferiche virtuali.
- Blocca le connessioni dei componenti spyware con il server che li controlla.
- Non permette ai malware di compromettere le routine di sistema, quali i backup pianificati.

### Requisiti di sistema

- Windows 10/8/8.1/7/Vista SP2/XP SP2+ (a 32 bit)
- Windows 10/8/8.1/7/Vista SP2 (a 64 bit)
- RAM: almeno 512 MB.
- Spazio libero su disco: ~150 MB. I file temporanei creati durante l'installazione richiedono ulteriore spazio su disco.

## ► **Dr.Web Antivirus per OS X**

Protezione indispensabile contro i virus e altri malware scritti per infettare non solo OS X ma anche altri sistemi operativi

Questo prodotto è disponibile come parte delle licenze Dr.Web Security Space e Dr.Web Antivirus.

### **Vantaggi**

- La scansione asincrona consente all'utente di eseguire istantaneamente qualsiasi azione con qualsiasi tipo di file – un basso consumo delle risorse di sistema rende il funzionamento di Dr.Web Antivirus per OS X quasi impercettibile.
- In Dr.Web per OS X la scansione di un file non blocca mai il sistema operativo, anche se un errore occorre durante la scansione.
- Nella maggior parte dei casi, funzionando con le importazioni predefinite, l'antivirus non richiede alcuna partecipazione da parte dell'utente e non lo distrae dai compiti attuali.
- Lo stile Apple OS X Aqua utilizzato nell'interfaccia di Dr.Web rende l'utilizzo chiaro e semplice.

### **Funzioni**

- Vengono scansionati oggetti in esecuzione automatica, dispositivi rimovibili, dischi logici e cartelle condivise, formati di email, file e cartelle, compresi file pacchettati e archivi compressi
- Tipo di scansione: rapida, completa e personalizzata
- Scansione antivirale avviata manualmente, automaticamente o secondo un calendario impostabile
- Le impostazioni del monitor SpIDer Guard® sono protette da password contro modifiche non autorizzate
- A oggetti infetti, sospetti o altri si applicano azioni, tra cui cura, spostamento in quarantena ed eliminazione la quale si applica anche quando l'azione selezionata come prima non può essere applicata all'oggetto
- Possibilità di escludere da scansione file e cartelle desiderati
- Rileva e rimuove virus nascosti sotto packer sconosciuti
- Si registrano il tempo di un evento, l'oggetto scansionato e il tipo di azione applicato all'oggetto
- Scaricamento di aggiornamenti in maniera automatica (secondo un calendario) o a richiesta
- Avvisi automatici (anche tramite segnali sonori) informanti di eventi virali
- File infetti vengono isolati in quarantena e si possono definire il tempo di conservazione degli oggetti in quarantena e la dimensione massima della cartella di quarantena
- Oggetti spostati in quarantena possono essere curati, ripristinati o rimossi
- Log dettagliato
- I moduli dell'antivirus sono disponibili come utility da riga di comando e possono essere incorporati in Apple Scripts

### **Requisiti di sistema**

- OS X 10.7 e superiore
- Memoria operativa – in conformità ai requisiti del SO
- Accesso a Internet per registrare una licenza e per ricevere aggiornamenti

### **Link utili**

Descrizione: <http://products.drweb.com/mac/>

## ► **Dr.Web Antivirus per Linux**

Protezione indispensabile contro i virus

### **Funzionalità principali**

- Rileva e neutralizza i virus e gli oggetti maligni sui dischi rigidi e supporti rimovibili.
- Riconosce i virus negli archivi di tutti i livelli gerarchici e negli oggetti compressi.

- Verifica i file compressi dai programmi di compressione, anche da quelli sconosciuti, tramite la tecnologia FLY-CODE.
- Protegge contro le minacce sconosciute tramite la tecnologia della ricerca non basata su firme anti-virali Origins Tracing e l'analizzatore intellettuale euristico Dr.Web.
- Scansione rapida, completa, selettiva oppure personalizzata.
- Esamina di continuo lo stato del computer – intercetta "al volo" gli accessi ai file sui dischi, dischetti, CD/DVD/Blu-ray, schede di memoria.
- Difende i propri elementi dai tentativi dei codici maligni di impedire il loro funzionamento.
- Isola gli oggetti infetti nella quarantena e rende possibile recuperarli; si può limitare la dimensione della quarantena.
- Raccoglie tutti i dati statistici sul funzionamento dell'antivirus.
- Carica gli aggiornamenti automaticamente secondo il calendario oppure su richiesta.

### Vantaggi

- Centro di controllo comodo.
- Possibilità del controllo "al volo".
- Le impostazioni di controllo possono essere personalizzate dall'utente.
- Quarantena gestibile.
- Aggiornamenti automatici.
- Interfaccia moderna.

### Requisiti di sistema

- Sistema operativo: distribuzioni GNU/Linux che funzionano sulla piattaforma Intel x86/amd64 sulla base del kernel 2.6.37 (e superiori) e utilizzano la libreria glibc versione 2.13 (e superiori).
- Almeno 512 MB di spazio su disco rigido.
- Accesso alla rete Internet per la registrazione e l'ottenimento di aggiornamenti.

### Link utili

Descrizione: <http://products.drweb.com/linux/>

## ► **Dr.Web Scanner a linea di comando**

Protezione antivirus con possibilità ampliate dell'automatizzazione per gli utenti esperti

Gli scanner Dr.Web a linea di comando senza l'interfaccia grafica usano il comune database di virus e il modulo di ricerca Dr.Web e sono progettati per i sistemi operativi MS DOS, OS/2 e Windows. Per gestire la protezione antivirus si deve avere l'esperienza del lavoro con la linea di comando.

### Vantaggi

- Requisiti di sistema minimi – gli scanner funzionano bene persino nei sistemi incorporati e sono in grado di proteggere efficacemente i computer di piccola potenza delle generazioni precedenti.
- Controllo conveniente – l'amministratore può scegliere la scansione "a mano" oppure la verifica secondo il calendario.
- Pulisce le workstation e i server infettati, anche quelli inaccessibili attraverso la rete.
- Molto resistente ai virus, può essere installato direttamente sul computer infettato.
- Le operazioni di ogni giorno possono essere automatizzate mediante le capacità abbondanti della linea di comando.
- Garantisce l'eliminazione dei virus sconosciuti per Dr.Web o compressi in archivi di formati sconosciuti.
- Può essere avviato da qualsiasi supporto rimovibile (da CD o chiavetta USB).

### Link utili

Descrizione: <http://products.drweb.com/console>

## ► Dr.Web Mobile Security

Protezione dei dispositivi mobili

### Componenti di protezione in Dr.Web Mobile Security

Componenti di protezione	Android	Symbian	Windows Mobile	BlackBerry
Antivirus	+	+	+	+
Antispam	+	+	+	
Antifurto	+			
Filtro URL	+			
Firewall	+			
Auditor della sicurezza	+			+

### Licenze di Dr.Web Mobile Security

1. Le licenze del prodotto vengono concesse sulla base del numero di dispositivi mobili protetti (1 – 5).
2. Le durate delle licenze commerciali: 12, 24 o 36 mesi. Le durate delle licenze OEM sono 3 o 6 mesi.
3. Non sono previsti alcuni sconti per questo prodotto, neanche gli sconti sul rinnovo. Per continuare a utilizzare il prodotto dopo la scadenza della licenza o per aumentare il numero di dispositivi protetti (cioè per fare un acquisto supplementare), è necessario acquistare una licenza nuova senza sconto.

## ► Dr.Web per Android

### Funzioni e vantaggi

- Scansione rapida o completa del file system, scansione di singoli file e cartelle a richiesta dell'utente.
- Controllo in tempo reale del file system che il monitor SpIDer Guard esegue al tentativo di salvare file nella memoria del dispositivo.
- Rilevamento dei programmi malevoli nuovi, non conosciuti ancora, tramite la tecnologia unica Origins Tracing™.
- Protezione della scheda SD contro i file di esecuzione automatica e contro Exploit.CpLink che possono mettere a rischio dispositivi Windows.
- Spostamento in quarantena di minacce rilevate con la possibilità di recuperare file spostati.
- Minimo effetto sulle prestazioni del sistema operativo.
- Risparmio della batteria.
- Risparmio della banda grazie a piccoli aggiornamenti dei database virali, il che è particolarmente importante in caso delle tariffe di telefonia con limite.
- Statistiche dettagliate sul funzionamento dell'antivirus.
- Funzionali e informativi widget per accedere all'applicazione dalla schermata principale.

### Antispam

Protegge da chiamate e SMS indesiderati.

- Scelta dei modi di filtraggio chiamate e SMS.
- Profili di filtraggio personalizzabili.
- Modifica della black list (per bloccare chiamate e SMS provenienti da alcuni numeri telefonici).
- Possibilità di vedere chiamate e SMS bloccati.

## Antifurto

Aiuta a trovare il dispositivo mobile in caso di smarrimento o furto e, se necessario, permette di cancellare su remoto le informazioni riservate.

- Blocco del cellulare dopo il riavvio.
- Blocco del cellulare più la richiesta di immettere la password di sblocco (il numero di tentativi immissione password è limitato).
- Sblocco del cellulare tramite un SMS.
- Ricezione delle coordinate GPS del cellulare come collegamento su Google Maps.
- Possibilità di cancellare informazioni su remoto dal cellulare e dalla scheda SD.
- Attivazione sul cellulare di un forte segnale acustico e blocco dello schermo.
- Impostazione di un testo personalizzabile da essere visualizzato sullo schermo del cellulare bloccato.
- Si può creare una lista dei numeri telefonici delle persone vicine che riceveranno avvisi di cambio della SIM card sul dispositivo smarrito. Da questi numeri è possibile gestire l'Antifurto e anche sbloccare il cellulare se il proprietario ha dimenticato la password.

## Filtro URL Cloud Checker

Il Filtro URL Cloud Checker basato sul cloud limita l'accesso a risorse di Internet indesiderate. L'accesso viene limitato alle seguenti categorie di siti sconsigliati e potenzialmente pericolosi:

- Droga.
- Fonti conosciute di virus.
- Linguaggio osceno.
- Terrorismo.
- Violenza.
- Armi.
- Siti per adulti ecc.

## ► Dr.Web per BlackBerry

### Funzioni e vantaggi

- Scansione rapida / completa del file system nonché la scansione di singoli file e cartelle on demand, la verifica della scheda di memoria, la verifica degli archivi.
- Controllo del file system in tempo reale eseguito dal monitor SpIDer Guard al tentativo di salvataggio dei file nella memoria del dispositivo e di installazione dei programmi.
- Protezione della scheda SD dall'infezione dai file di esecuzione automatica e dagli Exploit.CpInk che potrebbero mettere a rischio dispositivi Windows
- Risparmio di traffico grazie alle piccole dimensioni degli aggiornamenti dei database dei virus, il che è particolarmente importante in caso delle tariffe mobile limitate.
- Spostamento delle minacce rilevate in quarantena con la possibilità di recuperare da quarantena i file spostati.
- Minima influenza sulle prestazioni del sistema operativo.
- Risparmio della batteria.
- Statistiche dettagliate delle minacce rilevate, del funzionamento dell'antivirus, inoltre del log di registrazione di eventi.
- Diagnostica del dispositivo alla ricerca delle vulnerabilità. Aiuto nell'eliminare problemi della sicurezza e vulnerabilità del dispositivo.

# Dr.Web Enterprise Security Suite. Prodotti per l'impresa



**Dr.Web Enterprise Security Suite** è un gruppo di prodotti Dr.Web che comprende gli strumenti di protezione per tutte le unità di una rete aziendale e ha un unico centro di controllo per la maggior parte di essi.

I prodotti sono raggruppati secondo il tipo di oggetti da proteggere. Se il cliente ha delle richieste determinate, questo rende molto più facile la ricerca del prodotto adatto.

Prodotto	Programmi
<b>Dr.Web Desktop Security Suite</b> Protezione delle workstation, dei client di terminal server, dei client di server virtuali e dei client di sistemi incorporati	Dr.Web per Windows
	Dr.Web per Linux
	Dr.Web per OS X
	Dr.Web per MS DOS*
	Dr.Web per OS/2*
<b>Dr.Web Server Security Suite</b> Protezione dei file server e server di applicazioni (compresi terminal server e server virtuali)	Dr.Web per i Windows server
	Dr.Web per i UNIX server
	Dr.Web per i Novell NetWare server
	Dr.Web per i OS X Server
<b>Dr.Web Mail Security Suite</b> Protezione della posta elettronica	Dr.Web per gli UNIX mail server
	Dr.Web per MS Exchange
	Dr.Web per IBM Lotus Domino per Windows
	Dr.Web per IBM Lotus Domino per Linux
	Dr.Web per i Kerio mail server per Windows
	Dr.Web per i Kerio mail server per Linux
<b>Dr.Web Gateway Security Suite</b> Protezione dei gateway	Dr.Web per gli UNIX Internet Gateway*
	Dr.Web per i Kerio Internet Gateway
	Dr.Web per MIMESweeper*
	Dr.Web per Qbik WinGate*
	Dr.Web per Microsoft ISA Server e Forefront TMG*
<b>Dr.Web Mobile Security Suite</b> Protezione dei dispositivi mobili	Dr.Web per Windows Mobile
	Dr.Web per Symbian OS*
	Dr.Web per Android

\* Il pannello di controllo centralizzato non è stato ancora implementato.

## Come scegliere il prodotto giusto: l'algoritmo

1. Che cosa vuole proteggere?	2. Che sistema operativo / piattaforma gestisce gli oggetti da proteggere?*	3. Le occorre solo l'antivirus o la protezione integrata?	4. Quanti sono gli oggetti da proteggere?	5. Per quanto tempo serve la licenza?	6. La licenza richiesta è l'acquisto primario, il rinnovo, l'acquisto complementare, l'acquisto complementare e il rinnovo? Al cliente spetta qualche agevolazione?
Determiniamo il prodotto	Determiniamo SO / piattaforma	Determiniamo la licenza di base	Determiniamo il numero delle licenze	Determiniamo la durata della licenza	Determiniamo il tipo di licenza ed eventuali agevolazioni
Workstation (Dr.Web Desktop Security Suite)	<ul style="list-style-type: none"> <li>■ Windows 8/7 Vista/XP SP2/2000 SP4 + Rollup 1 (a 32 e 64 bit)</li> </ul>	<ul style="list-style-type: none"> <li>■ Protezione integrata</li> <li>■ Antivirus</li> </ul>	1...	12, 24 o 36 mesi	
	<ul style="list-style-type: none"> <li>■ OS X</li> <li>■ Linux</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> </ul>			
	MS DOS, OS/2				
File server (Dr.Web Server Security Suite)	<ul style="list-style-type: none"> <li>■ Windows</li> <li>■ Novell NetWare</li> <li>■ OS X Server</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> </ul>	1...		
	<ul style="list-style-type: none"> <li>■ UNIX</li> </ul>				
Traffico di posta elettronica (Dr.Web Mail Security Suite)	<ul style="list-style-type: none"> <li>■ UNIX</li> <li>■ MS Exchange</li> <li>■ Lotus Domino</li> <li>■ Kerio</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> </ul>	<ul style="list-style-type: none"> <li>■ Il numero illimitato di utenti</li> <li>■ Server con 3000 di utenti da proteggere</li> </ul>		
Traffico Internet (Dr.Web Gateway Security Suite)	<ul style="list-style-type: none"> <li>■ UNIX Internet Gateway</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> </ul>	<ul style="list-style-type: none"> <li>■ Il numero illimitato di utenti</li> <li>■ Server con 3000 utenti da proteggere</li> </ul>		
	<ul style="list-style-type: none"> <li>■ Kerio Internet Gateway</li> </ul>				
	<ul style="list-style-type: none"> <li>■ Qbik WinGate</li> </ul>				
	<ul style="list-style-type: none"> <li>■ MIMESweeper</li> </ul>				
	<ul style="list-style-type: none"> <li>■ Microsoft ISA Server e Forefront TMG</li> </ul>				
Dispositivi mobili (Dr.Web Mobile Security Suite)	<ul style="list-style-type: none"> <li>■ Android</li> </ul>	<ul style="list-style-type: none"> <li>■ Protezione integrata</li> </ul>	Il numero illimitato di dispositivi mobili		
	<ul style="list-style-type: none"> <li>■ Symbian</li> </ul>				
	<ul style="list-style-type: none"> <li>■ Windows Mobile</li> </ul>				

\* Questo passo è necessario solo quando scegliamo la protezione per le workstation, perché dal sistema operativo usato dipende l'assortimento disponibile degli elementi complementari della protezione (vedere "Licenze dei prodotti Dr.Web").

## ► Pannello di controllo Dr.Web

La gestione centralizzata della protezione di tutte le unità che compongono la rete aziendale

### Funzionalità principali

Gestisce nel modo centralizzato tutti gli elementi della protezione, esamina di continuo lo stato di tutte le unità protette della rete, è possibile impostare la reazione automatica sugli incidenti virus.

### Vantaggi

- Consente di gestire a bassi costi la protezione della rete aziendale da qualsiasi punto del mondo da una sola postazione di lavoro (tramite Amministratore Web), dovunque si sia, anche fuori della rete aziendale.
- Minimo costo complessivo in confronto ai programmi concorrenti grazie alla possibilità di svolgere le reti che girano sotto i server Windows e Linux, alla semplicità dell'installazione e all'affidabilità della protezione.
- Il sistema di protezione in sostanza può essere utilizzato in qualsiasi rete aziendale indipendentemente dalla sua dimensione e dalle sue caratteristiche quali il numero degli impiegati e delle filiali, la topologia, la disponibilità o meno del server Active Directory.
- Rende possibile utilizzare gli agenti sulle workstation in modo conveniente per l'amministratore – tramite i servizi di Active Directory, gli script di avvio, i mezzi per l'installazione da remoto. L'installazione è possibile, anche se l'unità della rete è chiusa e inaccessibile per il server antivirale.
- Rende possibile realizzare gli approcci di sicurezza individuali concreti per l'azienda.
- L'operazione si può automatizzare grazie all'integrazione con il sistema Windows NAP.
- Scalabilità straordinaria adatta per le reti di qualsiasi dimensione e qualsiasi complessità. La scalabilità è resa possibile perché si usa la gerarchia dei server antivirali interagenti del Pannello di Controllo e il server SQL separatamente usato per l'immagazzinamento di dati, e anche perché vi è la struttura complessa dell'interazione tra essi e le unità protette della rete.
- La trasmissione di dati tra gli elementi del sistema avviene in modo sicuro grazie alla possibilità di codificazione.
- Minimo traffico Internet. I dati scambiati tra il client e il server sono compressi tramite un protocollo di scambio dati appositamente creato.
- Operazioni trasparenti – il registro di verifica delle azioni degli amministratori consente di rintracciare tutti i passi dell'installazione e della configurazione del sistema. Tutti i suoi elementi sono in grado di mantenere i file di rapporto nei quali si possono impostare i dettagli di specifica.
- Ha un meccanismo comodo di avvertimento all'amministratore sui problemi verificatisi nella rete antivirale.
- C'è la possibilità di designare amministratori separati per gruppi diversi, il che consente di usare il Pannello di Controllo sia nelle aziende con i requisiti di sicurezza aumentati, sia nelle aziende con tante filiali.
- Si possono configurare approcci di sicurezza per diversi tipi di utenti, inclusi "utenti mobili", e per ogni tipo di workstation, anche quelle assenti dalla rete in un dato momento, il che consente di assicurare lo stato aggiornato della protezione in qualunque momento.
- Assicura che le impostazioni di protezione non possano essere cambiate dagli utenti.
- Possibilità di proteggere le reti che non hanno l'accesso a Internet.
- Possibilità di usare la maggioranza dei database esistenti, sia interni, che esterni. I database esterni possono essere Oracle, PostgreSQL, Microsoft SQL Server, qualsiasi DBMS con il supporto di SQL-92 tramite ODBC.
- Possibilità di scrivere i propri gestori di eventi su qualsiasi linguaggio scripting, il che consente l'accesso diretto alle interfacce interne del Pannello di Controllo.

- Possibilità di dare addietro un aggiornamento – l'unità della rete non rimane senza protezione, anche se il processo d'aggiornamento ha causato un errore.
- L'apertura – per mezzo del Pannello di Controllo l'amministratore di sistema può installare e sincronizzare programmi aggiuntivi di altri produttori, il che riduce anche i costi per la costruzione di sistemi di sicurezza informatica.
- Il sistema del controllo sullo stato della protezione è molto chiaro, la ricerca delle workstation della rete è insuperabile per efficienza e comodità.
- Le possibilità di scegliere l'elenco degli elementi del prodotto da aggiornare e di controllare la migrazione sulle nuove versioni consentono agli amministratori di installare solamente gli aggiornamenti necessari e verificati nella loro rete.

#### **Link utili**

Servizio di prova online Dr.Web LiveDemo: [http://download.drweb.com/live\\_demo/](http://download.drweb.com/live_demo/)

## ► Dr.Web Desktop Security Suite

La protezione delle workstation, dei client di terminal server, dei client di server virtuali e dei client di sistemi incorporati.

- Dr.Web per Windows
- Dr.Web per Linux
- Dr.Web per OS X
- Dr.Web scanner a linea di comando per Windows, MS DOS, OS/2

### Sistemi operativi supportati

Dr.Web per Windows	Dr.Web per Linux	Dr.Web per OS X	Dr.Web scanner a linea di comando
Windows 2012/8/7/2008/ Vista/2003/XP SP 2 (sistemi a 32 e 64 bit)	Distribuzioni GNU/Linux che funzionano sulla piattaforma Intel x86/amd64 sulla base del kernel 2.6.37 (e superiori) e utilizzano la libreria glibc versione 2.13 (e superiori)	OS X 10.7 e superiore	Windows, MS DOS, OS/2

## Licenze di Dr.Web Desktop Security Suite

### Tipi di licenze

I tipi di licenze si distinguono secondo il numero delle workstation, dei client connessi al terminal server o dei client dei sistemi incorporati.

I prodotti Dr.Web Desktop Security Suite possono acquistarsi separatamente o come una parte del gruppo Dr.Web Enterprise Security Suite. Nell'ultimo caso si acquistano anche le licenze del Pannello di Controllo di Dr.Web Enterprise Security Suite (tranne gli scanner a linea di comando).

### Varianti di licenze

	Windows 8/7/Vista	Windows 8/7/Vista/XP/2000 SP4 + Rollup 1	Linux	OS X	MS DOS, OS/2
Licenza di base	Protezione integrata	Antivirus Windows 8/7/Vista/XP/2000 SP4 + Rollup 1 (a 32 e 64 bit)			
Elementi protettivi della licenza di base	<ul style="list-style-type: none"> <li>■ Antivirus</li> <li>■ Antispyware</li> <li>■ Antirrootkit</li> <li>■ Antispam</li> <li>■ Antivirus web</li> <li>■ Controllo d'ufficio</li> <li>■ Firewall</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> <li>■ Antispyware</li> <li>■ Antirrootkit</li> <li>■ Firewall</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> <li>■ Antispyware</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> <li>■ Antispyware</li> <li>■ Antirrootkit</li> </ul>	<ul style="list-style-type: none"> <li>■ Antivirus</li> <li>■ Antispyware</li> <li>■ Antirrootkit</li> </ul>
<b>Elementi complementari</b>					
Pannello di controllo	+	+	+	+	-

I prodotti che fanno parte di Dr.Web Desktop Security Suite (tranne gli scanner a linea di comando) sono disponibili anche nei pacchetti economici Dr.Web destinati alle piccole e medie aziende.

L'informazione sui prodotti software Dr.Web per Windows, OS X, Linux e sugli scanner a linea di comando si trova nella sezione Dr.Web Home Security Suite. Prodotti per uso domestico. Le informazioni sul prodotto Dr.Web Security Space corrispondono alla licenza di Protezione Integrata.

## ► Dr.Web Server Security Suite

La protezione dei file server e dei server di applicazioni (inclusi i terminal server)

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

### Sistemi operativi supportati

Dr.Web per Windows server	Dr.Web per UNIX server	Dr.Web per Novell NetWare server	Dr.Web per OS X Server
Microsoft Windows Server 2000* / 2003 (x32 & x64*) / 2008 / 2012 (x64)	<ul style="list-style-type: none"> <li>■ Linux versione del nucleo 2.4.x e superiore</li> <li>■ FreeBSD versione 6.x e superiore per la piattaforma Intel x86</li> <li>■ Solaris versione 10 per la piattaforma Intel x86</li> </ul>	Novell NetWare versione 4.11 – 6.5	OS X Server 10.7 e superiore

\* Vengono supportati solo per la versione 7.0.

I prodotti Dr.Web Server Security Suite possono acquistarsi separatamente o come una parte del gruppo Dr.Web Enterprise Security Suite. Nell'ultimo caso si acquistano anche le licenze del Pannello di Controllo di Dr.Web Enterprise Security Suite (tranne i server UNIX).

	Dr.Web per Windows server	Dr.Web per Novell NetWare server	Dr.Web per UNIX server	Dr.Web per OS X Server
Licenza di base	Antivirus			
<b>Elementi complementari</b>				
Pannello di controllo	+	+	+	+

I prodotti che fanno parte di Dr.Web Server Security Suite sono disponibili anche nei completi economici Dr.Web destinati alle piccole e medie aziende.

## ► Dr.Web per Windows Server

La protezione antivirus dei file server e terminal server che girano sotto Windows, inclusi i server di applicazioni

### Vantaggi

- Si può usare negli enti che richiedono il massimo grado di protezione poiché il prodotto è completamente conforme alle leggi russe e ha i certificati di approvazione del Servizio Federale di Controllo Tecnico e d'Esportazione e del Servizio Federale di Sicurezza della Russia.
- Alto rendimento e funzionamento stabile.
- Alta velocità di scansione e minimo peso sul sistema operativo, il che mette Dr.Web in grado di funzionare su server aventi pressoché ogni configurazione.
- Funzionamento continuo dell'antivirus in modo automatico.

- Distribuisce flessibilmente il carico sul sistema file del server grazie alla tecnologia unica del controllo differito dei file aperti "per la lettura".
- Ha una struttura d'impostazioni flessibile e orientata sui client nella quale si può scegliere gli oggetti da controllare, le azioni da eseguire in caso se si individuano virus o file sospetti.
- Il programma è facile da installare e da gestire.
- Garantisce una protezione di assoluto valore subito dopo l'installazione (con le impostazioni predefinite).
- Trasparenza – genera i file di rapporti dettagliati con i dati richiesti dall'amministratore.

### Funzionalità principali

- Verifica i volumi del server secondo il calendario prestabilito o su richiesta dell'amministratore.
- Scansione fatta "al volo" – direttamente quando i file sono memorizzati oppure aperti sul server dalle workstation.
- Controllo a molteplici thread.
- Avviso istantaneo dell'amministratore, di altri utenti e gruppi sugli incidenti virus – via email oppure tramite un messaggio inviato al numero telefonico.
- I file infetti sono isolati in quarantena.
- Pulisce, recupera e/o elimina i file messi in quarantena.
- Mantiene il registro delle attività antivirus.
- I database dei virus si aggiornano automaticamente.
- Possibilità di eliminare minacce già nel corso dell'installazione
- Risparmia risorse del sistema e tiene presente le prestazioni dell'hardware
- Velocità di scansione massima grazie alla tecnologia multi-thread e alla regolazione del tasso di utilizzo delle risorse server
- Un sistema di notifica che non distrae l'utente con numerosi avvisi\*
- Dr.Web Cloud – una reazione istantanea a minacce più recenti\*
- Protezione preventiva – una difesa affidabile da minacce ancora non conosciute che proibisce modifiche degli oggetti critici di Windows e controlla azioni non sicure\*
- Sottosistema di scansione in background e di neutralizzazione di minacce attive – Dr.Web per Windows può eliminare qualsiasi minaccia anche una particolarmente tenace
- Gestione degli antivirus Dr.Web per Windows nella rete locale da qualsiasi dei computer senza installare il Pannello di controllo Dr.Web
- Esegue una scansione rapida/completa/personalizzata della memoria operativa, dei dischi, di unità logiche, CD, cartelle condivise, cartelle locali, file, mail file, settori di avvio e di altri oggetti del sistema

### Requisiti di sistema

- Processore: supporta l'insieme d'istruzioni i686 e superiore.
- Sistema operativo: Microsoft Windows Server 2000\*\* / 2003 (x32 & x64\*\*) / 2008 / 2012 (x64)
- Memoria operativa: 512 MB e più.

### Link utili

Descrizione: <http://products.drweb.com/fileserver/win>

---

\* Vengono supportati solo per la versione 7.0.

\*\* Disponibile per i sistemi operativi Windows Server 2008 o superiori.

## ► Dr.Web per OS X Server

La protezione antivirus delle workstation che girano sotto le versioni server del sistema operativo OS X

### Funzionalità principali

- Verifica gli oggetti di avvio automatico, i supporti rimovibili, le cartelle condivise e i volumi, i formati di posta, i file e le cartelle anche quelli impacchettati e compressi in archivi.
- Scansione rapida, completa e selettiva.
- Controllo di virus eseguito a mano, automaticamente o secondo il calendario prestabilito.
- Protegge con password le impostazioni del monitor SplDer Guard contro la modificazione non autorizzata.
- Applicazione delle azioni per gli oggetti infetti, sospettabili e di altro tipo, inclusi la pulitura, lo spostamento in quarantena e l'eliminazione, anche se l'azione scelta prima si sia verificata impossibile.
- Si possono escludere dalla verifica i percorsi e i file richiesti dall'utente.
- Rilevamento ed eliminazione dei virus nascosti da un programma di compressione sconosciuto.
- Registra il tempo di un evento, l'oggetto controllato e il tipo dell'azione eseguita.
- Carica gli aggiornamenti automaticamente (secondo il calendario) oppure su richiesta.
- Avvisi automatici (anche con l'uso dell'avvertimento sonoro) sugli eventi di virus.
- Isola i file infetti in quarantena e consente di impostare la durata della manutenzione d'oggetti in quarantena e la dimensione massima della quarantena.
- Pulisce, recupera oppure elimina gli oggetti spostati in quarantena.
- Mantiene rapporti dettagliati sulla sua operazione.
- I moduli sono accessibili sotto forma di utilità a linea di comando e possono essere incorporati nei sistemi di servizio Apple Scripts.

### Vantaggi

- Comodo Centro di controllo.
- Alta velocità di scansione.
- Possibilità di creare profili di scansione personalizzati.
- Protezione affidabile in tempo reale.
- Peso minimo sulle risorse del sistema protetto.
- Consumo minore di traffico durante la ricezione degli aggiornamenti.
- Molteplici impostazioni.
- Facile da gestire.
- Interfaccia moderna e comoda.

### Requisiti di sistema

- OS X Server 10.7 e superiore.
- Processore Intel.
- Memoria operativa – a seconda dei requisiti del SO.
- L'accesso a Internet per registrare il prodotto e ricevere gli aggiornamenti.

### 🔗 Link utili

Descrizione: <http://products.drweb.com/filesserver/mac>

## ► Dr.Web per Novell NetWare Server

La protezione antivirus dei depositi di file

### Funzionalità principali

- Verifica i volumi di server secondo il calendario prestabilito oppure su richiesta dell'amministratore.
- Controlla "al volo" tutti i file che passano attraverso il server.
- Controllo a molteplici thread.
- Rende possibile regolare il grado del carico del processore, il che consente di impostare la priorità del processo di scansione nel sistema.
- La workstation dalla quale sorge una minaccia di virus viene automaticamente scollegata dal server.
- La verifica viene protocollata; il livello di dettagli del protocollo è configurabile.
- Avvisi del rilevamento d'oggetti infettati.
- Pulisce, elimina gli oggetti infettati o li sposta in quarantena.
- L'antivirus si gestisce dal pannello del server o dal pannello remoto.
- Mantiene la statistica delle scansioni e il registro delle attività dell'antivirus.
- I database dei virus si aggiornano automaticamente.

### Vantaggi

- Una gamma ampia delle versioni di Novell NetWare supportati – dalla 4.11 alla 6.5.
- Supporta lo spazio dei nomi NetWare.
- Scansione dei vasti flussi di dati ad alta velocità con il carico minimo sul sistema operativo.
- Facile da installare.
- Ha una struttura d'impostazioni flessibile e orientata sui client nella quale si possono impostare i parametri del controllo e le azioni da eseguire in caso si individuino dei codici maligni.

### Requisiti di sistema

- Novell NetWare delle versioni 4.11–6.5. con i supplementi dal Minimum patch list.

### ☀ Link utili

Descrizione: <http://products.drweb.com/fileserver/novell>

## ▶ Dr.Web per UNIX Server

Protezione antivirus di file server Unix

### Vantaggi

- Alto rendimento e funzionamento stabile.
- Alta velocità di scansione e minimo peso sul sistema operativo, il che mette Dr.Web in grado di funzionare sui server pressoché in ogni configurazione.
- Ha una struttura d'impostazioni flessibile e orientata sui client nella quale si possono scegliere gli oggetti da controllare, le azioni da eseguire in caso se sono stati trovati dei virus o dei file sospetti.
- Ottima compatibilità – non entra in conflitto con nessun firewall o monitor di file conosciuti.
- Supporto dei sistemi di monitoraggio (Cacti, Zabbix, Munin, Nagios ecc.)
- Gestione conveniente, il programma è facile da installare e da configurare.

### Funzionalità principali

- Verifica i volumi di server secondo il calendario prestabilito oppure su richiesta dell'amministratore.
- Migliorato! La scansione fatta "al volo" – direttamente quando i file sono memorizzati oppure aperti sul server dalle workstation.
- Controllo a molteplici thread.
- La workstation dalla quale sorge una minaccia di virus viene automaticamente scollegata dal server.
- Avviso istantaneo dell'amministratore, di altri utenti e gruppi sugli incidenti virus – via email oppure tramite un messaggio inviato al numero telefonico.
- Migliorato! I file infetti sono isolati in quarantena.
- Pulisce, recupera e/o elimina i file messi in quarantena.
- Mantiene il registro delle attività antivirus.
- I database dei virus si aggiornano automaticamente.

### Requisiti di sistema

- Samba 3.0. e superiore.

### Sistemi operativi supportati

- GNU/Linux (sulla base del kernel di una versione non inferiore a 2.6.37 e con utilizzo della libreria glibc versione 2.13 e superiori);
- FreeBSD;
- Solaris – soltanto per le piattaforme Intel x86/amd64.

I sistemi operativi in uso devono utilizzare il server Samba di una versione non inferiore a 3.0 e il meccanismo di autenticazione PAM.

Se viene utilizzata una versione del sistema operativo a 64 bit, deve essere attivato il supporto di esecuzione di applicazioni a 32 bit.

Spazio su disco rigido:

- Almeno 1 GB

Il funzionamento del complesso è stato testato sulle distribuzioni:

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

### Link utili

Descrizione: <http://products.drweb.com/filesserver/unix>

## ► Dr.Web Mail Security Suite

La protezione della posta elettronica

- Dr.Web per UNIX mail server
- Dr.Web per MS Exchange
- Dr.Web per IBM Lotus Domino (Windows, Linux)
- Dr.Web per Kerio mail server (Windows, Linux)

### Sistemi operativi supportati

Prodotto Dr.Web	Windows	Linux	FreeBSD	Solaris
		per la piattaforma Intel x86		
Dr.Web per UNIX mail server		con la versione del nucleo 2.4.x e superiore	la versione 6.x e superiore	la versione 10
Dr.Web per MS Exchange	Server 2000 / 2003 / 2008 / 2012			
Dr.Web per IBM Lotus Domino	Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 (a 32 e 64 bit)	Red Hat Enterprise Linux (RHEL) delle versioni 4 e 5, Novell SUSE Linux Enterprise Server (SLES) delle versioni 9 e 10 (solo a 32 bit)		
Dr.Web per Kerio mail server	2000/XP/Vista/7, Server 2003/2008/2012	Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0, 11.1; CentOS Linux 5.2, 5.3; Debian 5.0; Ubuntu 8.04 LTS		

## Licenze di Dr.Web Mail Security Suite

### Tipi di licenze

- Licenza secondo il numero degli utenti protetti (illimitato).
- Licenza per un server – si può controllare la quantità illimitata della posta su un server con il numero degli utenti protetti 3 000 al massimo.

I prodotti Dr.Web per la protezione della posta elettronica possono acquistarsi separatamente o come una parte del gruppo Dr.Web Enterprise Security Suite. Nell'ultimo caso si acquistano anche le licenze del Pannello di Controllo di Dr.Web Enterprise Security Suite, il modulo Antispam e SMTP proxy.

L'uso congiunto dei prodotti per la protezione della posta elettronica e dell'elemento complementare SMTP proxy non solo aumenta la sicurezza generale della rete, ma riduce anche il carico sui server di posta interni e sulle workstation.

### Varianti di licenze

	Dr.Web per MS Exchange	Dr.Web per IBM Lotus Domino	Dr.Web per UNIX mail server	Dr.Web per Kerio mail server
Licenza di base	Antivirus			
<b>Elementi complementari</b>				
Antispam	+	+	+	
SMTP proxy	+	+	+	+
Pannello di controllo	+	+	+	+

I prodotti Dr.Web per la protezione della posta elettronica sono disponibili anche nei pacchetti economici Dr.Web destinati alle piccole e medie aziende.

## ► Dr.Web per UNIX mail server

La protezione antivirus e antispam del traffico di posta elettronica trasmesso attraverso i server gestiti da UNIX (Linux/FreeBSD/Solaris(x86))

### Funzionalità principali

- Filtraggio dei messaggi email alla ricerca dei virus e dello spam.
- Scomponi i messaggi email e ne analizza tutte le parti.
- Elaborazione corretta della maggioranza dei tipi d'archivi conosciuti, compresi gli archivi a molteplici volumi e archivi autoestraenti (SFX).
- Black lists e White lists.
- Avvisi impostabili.
- Mantiene la statistica che comprende tutti gli aspetti del funzionamento del sistema.
- Difende i propri moduli dai guasti.

### Conformità alla legge russa

Dr.Web per UNIX mail server ha i certificati di approvazione rilasciati dal Servizio Federale di Sicurezza e dal Servizio Federale di Controllo Tecnico e d'Esportazione della Russia. Pertanto il prodotto può essere usato negli enti che richiedono il grado di protezione elevato, ivi compreso come parte del sottosistema di protezione antivirale nei sistemi informatici dei dati personali della classe K1. La possibilità di archiviare tutti i messaggi email consente di usare questo prodotto come parte dei sistemi informatici degli istituti di credito.

### Possibilità di configurare il programma nel modo flessibile secondo le esigenze dell'utente

Si possono utilizzare delle regole per la configurazione di Dr.Web per UNIX mail server. Questa possibilità aumenta notevolmente la flessibilità del prodotto e lo distingue dai programmi concorrenti nei quali per la configurazione si usano i parametri statici del file di configurazione. I messaggi vengono filtrati e modificati in base alle politiche in uso. Inoltre l'amministratore può impostare le regole di elaborazione separate non solo per i diversi utenti e gruppi, ma anche in sostanza per ogni messaggio. Grazie a questo, il prodotto è in grado di corrispondere a tutti i requisiti aziendali della sicurezza informatica, il che ottiene un'importanza particolare dopo l'entrata in vigore della legge sulla protezione dei dati personali.

### Non richiede un alto livello professionale dell'amministratore

Nonostante la ricchezza delle funzionalità, Dr.Web per UNIX mail server non richiede di essere configurato a lungo prima di essere messo in esercizio. Questo prodotto è inoltre disponibile non solo come software, ma anche come l'insieme di software e dispositivi Dr.Web Office Shield, cioè un server progettato per il lavoro secondo il principio "una volta messo lo si è dimenticato".

### Alta velocità di risposta

La tecnologia di controllo a molteplici thread assicura l'alta velocità di risposta del sistema. In ogni caso i messaggi sono controllati "al volo", parallelamente all'elaborazione dei file presi prima. Questo consente agli utenti di ricevere la posta in modo immediato.

### Vantaggi aggiuntivi di Dr.Web Antispam:

- non richiede di essere istruito e comincia ad operare efficacemente dal momento dell'installazione – in confronto ai programmi antispam costruiti con l'algoritmo bayesiano (quali Panda, Kaspersky);
- la decisione su "è spam / non è spam" presa dal programma non dipende dalla lingua del messaggio;

- permette di assegnare diverse azioni per le varie categorie dello spam;
- usa le proprie black lists e white lists, il che rende impossibile compromettere le aziende inserendo con una mala intenzione i loro indirizzi nelle liste di indirizzi indesiderati;
- commette pochissimi errori di riconoscimento di spam;
- ha bisogno degli aggiornamenti non più di una volta al giorno – le tecnologie uniche di riconoscimento dei messaggi indesiderati basate su migliaia di regole liberano dalla necessità di scaricare spesso degli aggiornamenti voluminosi.

### Protezione delle informazioni riservate

Il prodotto permette di recuperare i messaggi che gli utenti hanno rimosso per inavvertenza dalle loro cassette postali e di fare indagini riguardanti la fuga d'informazioni. Ciò è anche agevolato dalla gestione della quarantena sia tramite l'interfaccia web, sia tramite un'utilità apposita, e dalla possibilità di archiviare tutti i messaggi trasmessi.

### Comodità dell'amministrazione

Il prodotto rende possibile l'uso dell'interfaccia web per impostare e gestire il programma e rende facile l'amministrazione della protezione da qualsiasi punto del mondo.

### Apertura

Dr.Web per UNIX mail server può essere integrato nelle soluzioni di altri produttori. Inoltre, grazie all'API (Interfaccia di programmazione di applicazioni) aperta vi si possono aggiungere nuove funzionalità.

### Possibilità di collegare plugin di quantità illimitata

Dr.Web per UNIX mail server consente di ampliare le funzionalità in modo illimitato e qualsiasi plugin sviluppato funziona con tutti i MTA supportati.

### I plugin realizzati:

- Dr.Web è un plugin del controllo antivirus per mezzo del motore antivirus Dr.Web;
- vaderetro è un plugin che filtra la posta alla ricerca dello spam attraverso la propria libreria Vade Retro;
- headersfilter è un plugin che filtra i messaggi in base ai titoli.

### Sistemi operativi supportati

- File di distribuzione Linux con la versione del nucleo 2.4.x e superiore.
- FreeBSD della versione 6.x e superiore per la piattaforma Intel x86.
- Solaris della versione 10 per la piattaforma Intel x86.

## Dr.Web SMTP proxy

Il modulo Dr.Web SMTP proxy è un elemento del prodotto Dr.Web per UNIX mail server che può essere installato sia nella "zona smilitarizzata" (DMZ), sia all'interno della struttura della posta. Poiché il server che verifica i messaggi email può essere trasferito nella "zona smilitarizzata" e il server di email può essere isolato da Internet, il malintenzionato non accederà alle informazioni importanti dell'azienda anche nel caso di intrusione sul server. La soluzione realizza il completo controllo della posta elettronica trasmessa attraverso i protocolli SMTP/LMTP.

### L'uso di Dr.Web SMTP proxy:

- sostanzialmente incrementa la sicurezza generale della rete;
- rende possibile migliorare notevolmente il filtro dei messaggi a causa dell'assenza di limitazioni imposte dai server di posta;
- riduce il carico sui server di posta interni e sulle workstation;
- incrementa in sostanza la stabilità del funzionamento del controllo di posta.

### Vantaggi

**Protezione contro gli attacchi di spammer** – per mezzo di Dr.Web SMTP proxy l'amministratore è messo in grado di limitare i parametri di una sessione SMTP e con questo di determinare i segni di un attacco di spammer.

**Autenticazione dell'indirizzo IP** – Dr.Web SMTP proxy consente di organizzare l'autenticazione di un indirizzo IP e proteggere l'azienda dallo spam mascherato sotto l'indirizzo IP di mittente inattendibile.

**Protezione contro gli attacchi di hacker** – Dr.Web SMTP proxy consente di resistere efficacemente sia agli attacchi "passivi" (del tipo PLAIN, LOGIN ecc.), sia agli attacchi attivi.

**Protezione contro le trappole di spam** – Dr.Web SMTP proxy consente di controllare il mittente per stabilire che non ci sia una trappola di spam.

**Protezione contro i messaggi formati incorrettamente** – Dr.Web SMTP proxy consente di bloccare i messaggi con campi di mittente vuoti però nello stesso tempo consente di elaborare correttamente i messaggi ricevuti dai client di posta che formano messaggi in modo errato.

**Risparmio del traffico Internet** – l'uso di Dr.Web SMTP proxy consente di risparmiare il traffico Internet e di impedire che gli allegati di misure enormi siano inviati da parte degli impiegati dell'azienda.

**Limitazione dei server Open Relay** – se l'azienda ha una necessità di organizzare un server Open Relay, con Dr.Web SMTP proxy l'amministratore può limitare l'elenco dei domini sui quali è permessa la trasmissione dei messaggi di posta.

### Link utili

Descrizione: <http://new-download.drweb.com/maild>

## ► **Dr.Web per MS Exchange**

La verifica antivirus e antispam del traffico trasmesso attraverso i server mail MS Exchange 2000/2003/2007/2010/2013/2016

### **Vantaggi**

- Possibilità di usare questo programma negli enti che richiedono un grado di protezione elevato poiché il programma è completamente conforme alle leggi russe e ha i certificati di approvazione rilasciati dal Servizio Federale di Sicurezza e dal Servizio Federale di Controllo Tecnico e d'Esportazione della Russia.
- Ci sono ampie possibilità di configurare e di impostare il programma in modo accurato secondo le esigenze dell'azienda.
- L'alta velocità di scansione e il minimo peso sul sistema operativo mettono Dr.Web in grado di funzionare benissimo sui server con qualsiasi configurazione.
- L'antispam incorporato che non richiede di essere istruito (comincia a operare dal momento dell'installazione) riduce notevolmente il carico sul server e aumenta la produttività lavoro degli impiegati dell'azienda.
- Il filtro in base alle black lists e white lists permette sia l'esclusione di certi indirizzi dalla verifica, sia l'incremento della sua efficienza.
- La possibilità di filtrare la posta secondo i tipi dei file consente all'azienda di diminuire il volume del traffico trasmesso.
- È disponibile la funzione del raggruppamento che rende possibile impostare diversi parametri per vari gruppi d'impiegati e pertanto aiuta a mettere in funzionamento più rapidamente il sistema di protezione antivirus e semplifica la sua manutenzione.
- I parametri di protezione si possono impostare flessibilmente tramite browser in modo conveniente per mezzo del pannello di controllo web dell'amministratore.
- Alto rendimento e funzionamento stabile grazie alla funzione del controllo a molteplici thread.
- Tecnologie uniche del rilevamento dei programmi di compressione e degli oggetti maligni sconosciuti (anche nuovissimi).
- L'applicazione si avvia del tutto automatico (con l'avvio del sistema operativo).
- Ricezione degli aggiornamenti comoda tramite lo schedulatore Windows.

### **Funzionalità principali**

- Verifica "al volo" i messaggi email, compresi i file allegati, alla ricerca di virus e spam.
- Monitoraggio antivirus dei messaggi trovati nelle cassette postali degli utenti e dei file memorizzati nelle cartelle condivise.
- Controllo antivirus del traffico postale di transito sul server MS Exchange.
- Pulisce i file infetti.
- Raggruppa gli utenti tramite Active Directory.
- Supporta la concezione dei ruoli del server e di agenti di trasporto per MS Exchange Server 2007/2010.
- Svolge la scansione con parametri prestabiliti: pertanto si può scegliere la misura massima e il tipo degli oggetti che vanno controllati, le azioni da compiere (anche le azioni da compiere con i file che non si prestano al controllo) e le modalità del trattamento degli oggetti infetti.
- Rileva i codici dannosi nascosti nei file che sono stati compressi in archivi a più riprese.
- Applica le varie azioni secondo il tipo dello spam, ivi compresi lo spostamento dei messaggi in quarantena e l'aggiunta del prefisso speciale all'oggetto del messaggio.
- Se è necessario, ai messaggi inviati si possono aggiungere testi spontanei.
- I file infetti o sospetti vengono isolati in quarantena.
- L'amministratore o gli altri utenti vengono avvisati degli incidenti virus.

- Il modulo mantiene i dati statistici del proprio funzionamento.
- Aggiornamenti automatici.

## Requisiti di sistema

### In caso si usa Microsoft Exchange Server 2000/2003:

- Processore Pentium a 133 MHz (consigliato quello a 733 MHz).
- Memoria operativa di 256 MB (consigliati 512 MB).
- Spazio libero sul disco: 20 MB per l'installazione; 50 MB per il registro di eventi.
- Microsoft Windows 2000 Server o Advanced Server con SP4 installato; Microsoft Windows Server 2003 (le versioni Standard, Enterprise oppure Datacenter) con SP1 installato e superiore.

### In caso si usa Microsoft Exchange Server 2007/2010:

- Processore Intel con l'architettura x64 che supporta la tecnologia Intel 64 o AMD che supporta la piattaforma AMD64.
- Memoria operativa di 2 GB.
- Spazio libero sul disco: 20 MB per l'installazione; 50 MB per il registro di eventi.
- Microsoft Windows Server 2003 R2 x64 con SP2 installato; Microsoft Windows Server 2008 x64.

### In caso si usa Microsoft Exchange Server 2013/2016:

- Processore Intel con l'architettura x64 che supporta la tecnologia Intel 64 o AMD che supporta la piattaforma AMD64.
- Memoria operativa di 4 GB.
- Spazio libero sul disco: 1 GB.
- Microsoft® Windows® Server 2008 R2; Microsoft® Windows® Server 2012; Microsoft® Windows® Server 2012 R2.

## Link utili

Descrizione: <http://products.drweb.com/mailserver/exchange>

## ► Dr.Web per IBM Lotus Domino

La protezione antivirus e antispam della piattaforma IBM Lotus Domino gestita da Windows e Linux

### Vantaggi

#### ■ Costo complessivo minimo

Dr.Web per IBM Lotus Domino funziona non solo sui server separati, ma anche sui server partitions e sui cluster Lotus Domino. Le copie dell'antivirus che si trovano nelle sezioni separate agiscono nella memoria del computer in modo autonomo usando i database e i file eseguibili comuni. In questo caso bisogna comprare la licenza di una sola copia, il che diminuisce sensibilmente i costi per la protezione antivirus.

#### ■ "Ready for IBM Lotus software"

Dr.Web per IBM Lotus Domino è stato incluso nella lista delle soluzioni IBM Lotus Business Solutions Catalog e gli è stato attribuito il logo "Ready for IBM Lotus software" a conferma che il nostro prodotto è compatibile con il sistema Lotus Domino e certifica che tutti i requisiti della compatibilità IBM sono stati esauditi.

#### ■ Alta velocità di scansione

Grazie all'organizzazione del sistema Dr.Web per IBM Lotus Domino, alla realizzazione speciale del modo di controllo e alla possibilità di gestire il controllo flessibilmente abbiamo ottenuto un'alta velocità di scansione con il minor consumo delle risorse del sistema operativo.

#### ■ Comodità di installazione e flessibilità delle impostazioni

Dr.Web per IBM Lotus Domino è abilitato a funzionare in modo automatico e facilmente gestibile. Il programma supporta gli script amministrativi e contiene la documentazione dettagliata. Il prodotto offre una gestione assai comoda grazie alla possibilità di configurarlo in modo flessibile tramite il pannello dell'amministratore. Si possono impostare in modo dettagliato le azioni che l'antivirus deve compiere in base ai risultati di una verifica, in particolare, il programma può spedire avvisi del rilevamento virus al mittente, al destinatario e agli amministratori del sistema, memorizzare i titoli dei messaggi email ricevuti nonché gli allegati, ecc.

#### ■ Agevolazione nell'amministrazione

L'amministrazione della protezione antivirus è alquanto facilitata dai meccanismi di raggruppamento e di gestione gruppi.

### Funzionalità principali

- Verifica e filtra "al volo" o sulla richiesta dell'amministratore i messaggi email e tutti i loro componenti alla ricerca dei virus, dello spam e della posta indesiderata.
- Filtra i messaggi alla ricerca di spam, usando in particolare le black lists e white lists.
- Controlla i virus nei documenti dei database NSF prestabiliti.
- Controllo degli oggetti a richiesta per mezzo della funzione dell'avvio e sospensione manuale dei compiti dello scanner.
- Scomposizione dei messaggi per la successiva verifica di tutte le loro parti.
- Pulizia dei messaggi infetti e dei file allegati.
- Rileva i codici dannosi nascosti nei file che sono stati compressi in archivi a più riprese.
- Utilizza il meccanismo del rilevamento dei codici dannosi nascosti dai programmi di compressione sconosciuti.
- Utilizza la tecnologia aggiuntiva del rilevamento dei codici dannosi sconosciuti la quale aumenta la probabilità che i virus di nuovissimo tipo siano rilevati.
- Mantiene gli oggetti infetti oppure sospetti in quarantena (agli oggetti spostati nella quarantena si può accedere tramite il client Lotus Notes).
- L'amministratore e altre persone vengono avvisati sui risultati di un controllo tramite i modelli descritti nel sistema, il che consente di ottenere le informazioni nel modo più conveniente possibile.
- Il programma mantiene i dati statistici del suo funzionamento.
- Difende i propri moduli dai guasti.
- Aggiornamenti automatici.

## Sistemi operativi supportati

### Versione per Windows

- Sistema operativo: Windows Server 2000/2003/2008/2008R2/2012/2012 R2 (versioni a 32 e 64 bit).
- Lotus Domino versione R6.0 e superiori (versioni a 32 e 64 bit).
- Processore Intel Pentium 133 e superiori.
- RAM 128 MB (consigliabile 512 MB).
- Spazio libero su disco: 128 MB.

### Versione per Linux

- Sistema operativo: Red Hat Enterprise Linux (RHEL) versione 4 e 5, Novell SuSE Linux Enterprise Server (SLES) versione 9 e 10 (solo a 32 bit).
- Lotus Domino versione 7.x o 8.x.
- Lotus Notes 6.5 (o successivo) per Windows.
- Processore Intel Pentium 133 e superiori.
- RAM 64 MB (consigliabile 128 MB).
- Spazio libero su disco: 90 MB.

### Link utili

Descrizione: <http://products.drweb.com/lotus>

## ▶ Dr.Web per Kerio mail server

Il controllo antivirus degli allegati di ogni messaggio email trasmesso attraverso i protocolli SMTP/POP3

### Vantaggi

- Il prodotto è perfettamente compatibile con i mail server Kerio, il che è stato comprovato dai testi Kerio Technologies.
- Offre la possibilità della protezione centralizzata per mezzo del Pannello di Controllo Dr.Web Enterprise Security Suite.
- Dr.Web è ora l'unico plugin antivirus russo adatto per i mail server Kerio, il che è molto importante nel caso delle consegne per gli enti pubblici.
- Impegna un tempo minimo per consegnare i messaggi e ha un grado di sicurezza elevato grazie alla tecnologia del controllo a molteplici thread.
- Risparmia le risorse del sistema operativo e non impone nessun peso sulla rete locale.
- Offre impostazioni flessibili e orientate ai clienti: si possono scegliere gli oggetti da controllare e le azioni che il modulo deve compiere nei riguardi dei virus e file sospetti.
- Possibile scegliere le azioni da compiere con i file che non si prestano al controllo.
- Gestione comoda tramite il pannello d'amministrazione del mail server Kerio.

### Funzionalità principali

- Controlla i file allegati a tutti i messaggi in entrata e in uscita.

## Sistemi operativi supportati

### Versione per Windows

- Spazio su disco rigido: almeno 350 MB
- Sistema operativo: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008/2012 (versioni a 32 e 64 bit)
- Mail server: Kerio MailServer 6.2 o superiori, Kerio Connect 7.0.0 o superiori.

### Versione per Linux

- Spazio su disco rigido: almeno 290 MB
- Sistema operativo: 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 e 11.1; CentOS Linux 5.2 e 5.3; Debian 5.0; Ubuntu 8.04 LTS.
- Mail server: Kerio MailServer 6.2 o superiori, Kerio Connect 7.0.0 o superiori.

### Versione per OS X

- Spazio su disco rigido: almeno 55 MB
- Sistema operativo: OS X 10.7 e superiori.
- Mail server: Kerio MailServer 6.2 o superiori, Kerio Connect 7.0.0 o superiori.

### Link utili

Descrizione: <http://products.drweb.com/mailserver/kerio>

## ► Dr.Web Gateway Security Suite

La protezione dei gateway

- Dr.Web per UNIX Internet Gateway
- Dr.Web per Kerio Internet Gateway
- Dr.Web per MIMESweeper
- Dr.Web per Qbik WinGate

### Sistemi operativi supportati

	Windows	Linux	FreeBSD	Solaris
		per la piattaforma Intel x86		
<b>Dr.Web per UNIX Internet Gateway</b>		con la versione del nucleo 2.4.x e superiore	la versione 6.x e superiore	la versione 10
<b>Dr.Web per Kerio Internet Gateway</b>	2000 / XP / 2003 / 2008 / 7			
<b>Dr.Web per MIMESweeper</b>	2000 Server SP4 e superiore / Server 2003 e superiore			
<b>Dr.Web per Qbik WinGate</b>	Vista / Server 2008 / Server 2003 / XP / 2000 (a 32 e 64 bit)			

## Licenze di Dr.Web Gateway Security Suite

### Tipi di licenze

- Licenza secondo il numero degli utenti protetti (illimitato).
- Licenza per un server – si può controllare una quantità illimitata del traffico su un server con massimo numero di 3.000 utenti protetti.

I prodotti Dr.Web per la protezione dei gateway possono acquistarsi separatamente o come una parte del gruppo Dr.Web Enterprise Security Suite. Nell'ultimo caso si acquistano anche le licenze del Pannello di Controllo di Dr.Web Enterprise Security Suite (solamente per Dr.Web per Kerio Internet Gateway) e il modulo Antispam (tranne UNIX e Kerio Internet Gateway).

### Varianti di licenze

	Dr.Web per UNIX Internet Gateway	Dr.Web per Kerio Internet Gateway	Dr.Web per MIMESweeper	Dr.Web per Qbik WinGate
Licenza di base	Antivirus			
<b>Elementi complementari</b>				
Antispam			+	+
Pannello di controllo	+	+		

I prodotti Dr.Web per la protezione dei gateway sono disponibili anche in pacchetti economici Dr.Web destinati alle piccole e medie aziende.

## ▶ Dr.Web per UNIX Internet Gateway

Il controllo antivirus del traffico HTTP e FTP trasmesso attraverso il gateway Internet aziendale – il server proxy

### Funzionalità principali

- Controllo antivirus del traffico HTTP e FTP.
- Gestione centralizzata tramite l'amministratore web del Pannello di Controllo di Dr.Web Enterprise Security Suite.
- Filtraggio dell'accesso secondo i tipi MIME e le dimensioni dei file oppure secondo il nome del nodo ospite.
- Regolazione dell'accesso alle risorse web.
- Ottimizzazione del controllo del traffico grazie all'uso della tecnologia Preview.
- Uso sia del protocollo IPv4, sia del protocollo della prossima generazione IPv6.
- Il programma controlla e applica diverse azioni a seconda dei tipi di file controllati.
- I file infetti vengono isolati in quarantena.
- Presenta i rapporti in modo appropriato.
- Elabora più richieste durante una connessione.
- Protegge dall'accesso non autorizzato.
- Monitoraggio e ripristino automatico del funzionamento del sistema.
- Avvisa l'utente dei tentativi di caricare una pagina dannosa o del rilevamento virus.

### Vantaggi

- Ampie possibilità di organizzare la protezione integrata contro le minacce nascoste nel traffico web entrante.
- Solo i contenuti sicuri vengono consegnati nella rete interna.
- Filtra il traffico efficacemente al livello del server ICAP e in sostanza senza alcun rallentamento nella consegna dei contenuti.
- Riduce notevolmente i costi dell'uso di Internet.
- Resiste in modo efficace alla penetrazione del malware di ogni tipo.
- Grande scalabilità – il modulo è in grado di elaborare in tempo reale flussi d'informazione enormi.
- Capacità di elaborare in tempo reale gli enormi flussi d'informazione.
- Compatibilità perfetta – si può integrare con qualsiasi software che supporta il protocollo ICAP (Internet Content Adaptation Protocol) e con tutti i firewall conosciuti.
- Supporta quasi tutti i sistemi operativi a base UNIX che sono oggi in uso.
- Richiede poche risorse del sistema operativo – il prodotto opera benissimo sui gateway Internet di quasi tutte le configurazioni.
- Flessibile e facile da amministrare – il prodotto permette di implementare quei modelli di protezione che corrispondono alle politiche di sicurezza dell'azienda.

### Sistemi operativi supportati

- Linux con la versione del nucleo 2.4.x e superiore.
- FreeBSD della versione 6.x e superiore (per la piattaforma Intel x86).
- Solaris della versione 10 (per la piattaforma Intel x86).

Qualunque server proxy che supporta pienamente il protocollo ICAP, in particolare:

- Squid di almeno 3.0.
- Shweby di almeno 1.0.
- SafeSquid di almeno 3.0.

### Link utili

Descrizione: <http://products.drweb.com/gateway/unix>

## ▶ Dr.Web per Kerio Internet Gateway

Il controllo antivirus del traffico trasmesso mediante i protocolli HTTP, FTP, SMTP e POP3 e mediante il servizio web Kerio Clientless SSL VPN

Dr.Web per Kerio Internet Gateway rappresenta un plugin antivirus che viene connesso al firewall Kerio. S'installa sullo stesso computer dove Kerio è già installato e viene usato da quest'ultimo come un software antivirus esterno.

### Vantaggi:

- Rileva gli oggetti malevoli trasmessi mediante i protocolli HTTP, FTP, SMTP e POP3 e mediante il service web Kerio Clientless SSL VPN.
- Protezione sicura dell'accesso a Internet sia per gli utenti privati, sia per le aziende di ogni dimensione e tipo di attività.
- Possibile la protezione centralizzata tramite il Pannello di Controllo di Dr.Web Enterprise Security Suite.
- Comodità dell'amministrazione – l'amministratore può ricevere gli avvisi di ogni incidente virus sia per email, sia per SMS.
- I messaggi vengono consegnati in tempi brevissimi grazie al controllo a molteplici thread.

### Funzionalità principali

- Rileva gli oggetti malevoli trasmessi mediante i protocolli HTTP, FTP, SMTP e POP3 e mediante il service web Kerio Clientless SSL VPN.
- Rileva gli allegati infetti nei messaggi di posta elettronica prima della loro elaborazione da parte del server mail.
- Forma l'elenco dei protocolli dello scambio d'informazioni che vengono controllati.
- Possibilità di controllare i dati del programma tramite il pannello web.
- Svolge la scansione con parametri prestabiliti: pertanto si può scegliere la misura massima e il tipo degli oggetti che vanno controllati e le modalità del trattamento dei file infetti.
- Avendo rivelato una minaccia, il programma applica le azioni secondo le impostazioni di Kerio.
- Attivazione / disattivazione del rilevamento del malware (secondo il tipo del malware).
- Registra gli errori ed eventi nel giornale di eventi (Event Log) e nel giornale di formato testuale.
- Spedisce le notifiche su vari eventi agli utenti prescelti.
- I database virus sono aggiornati in modo automatico.

### Requisiti di sistema

Versione per Windows

- Almeno 350 MB di spazio libero su disco.
- Sistema operativo Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (versioni a 32 e a 64 bit).
- Firewall Kerio WinRoute Firewall 6.2 e superiori, Kerio Control 7.0.0 e superiori.

Versione per Kerio Control VMware Virtual Appliance e Kerio Control Software Appliance

- Almeno 290 MB di spazio libero su disco.
- Sistema operativo Kerio Control VMware Virtual Appliance o Kerio Control Software Appliance.
- Firewall Kerio Control 8.x e superiori.

### Link utili

Descrizione: <http://products.drweb.com/gateway/kerio>

## ▶ **Dr.Web per MIMESweeper**

La protezione antivirus e antispam del traffico postale trasmesso attraverso i server di filtrazione contenuti ClearSwift MIMESweeper

### **Vantaggi**

#### **Semplice da installare e configurare**

I mezzi di configurazione incorporati in Dr.Web per MIMESweeper – che sono wizard di scenari – permettono di creare nel modo automatico gli scenari più moderni per il controllo di messaggi postali (il top secondo la classificazione ClearSwift).

#### **Compatibile con DEP**

Dr.Web per MIMESweeper supporta la tecnologia della prevenzione d'esecuzione dati (Data Execution Prevention, DEP) la quale è in grado di controllare la memoria e di pervenire l'esecuzione del codice. Grazie a questo supporto, gli utenti non devono cambiare il modo di operare DEP poiché i programmi malevoli non potranno sfruttare il meccanismo d'elaborazione esclusioni Windows.

#### **Impostazioni flessibili**

Avendo rivelato un oggetto infettato, il plugin Dr.Web cerca di pulirlo o lo rimuove subito se l'opzione di pulizia non è stata scelta. Se più file o archivi sono allegati a un messaggio postale, il plugin Dr.Web disinfecta solo gli allegati infetti. Se un virus è stato rivelato nel corpo di un messaggio, il filtro di contenuti sposta il messaggio in quarantena. I messaggi, file o archivi non infetti sono consegnati al destinatario senza alcune modifiche. I messaggi malevoli che il plugin Dr.Web non è capace di neutralizzare sono segnati e spostati in quarantena come impostazione predefinita.

### **Funzionalità principali**

- Verifica i messaggi postali e i loro allegati, anche gli archivi, prima della loro elaborazione da parte del server mail.
- Pulisce gli oggetti infettati.
- Isola i file infetti o sospetti in quarantena.
- Filtra la posta elettronica alla ricerca di spam, anche in base alle black lists e white lists.
- Mantiene i dati statistici della propria attività.
- Aggiornamenti automatici.

### **Requisiti di sistema**

- Sistema operativo Windows 2000 SP4 e superiore o Windows Server 2003 e superiore.
- Filtro di contenuti postali ClearSwift MIMESweeper per SMTP 5.2 e superiore.

### **🔗 Link utili**

Descrizione: <http://products.drweb.com/mimesweeper>

## ▶ **Dr.Web per Qbik WinGate**

Il controllo antivirus e antispam del traffico trasmesso mediante i protocolli HTTP/POP3/FTP del server proxy e del server SMTP Qbik Wingate

### **Funzionalità principali**

- Controllo antivirus e antispam dei messaggi email trasmessi mediante i protocolli SMTP e POP3 anche con la verifica dei file allegati.
- Controllo antivirus dei file e dati trasmessi mediante i protocolli HTTP e FTP.
- Pulisce i file infetti trasmessi mediante il protocollo HTTP.
- Mantiene il giornale di eventi.
- Ha il proprio pannello di controllo e il gestore della quarantena.
- Aggiornamenti automatici dei database dei virus.

### **Vantaggi**

- Solo Dr.Web per Qbik WinGate ha sia la documentazione, sia il supporto tecnico messi a disposizione direttamente dal produttore.
- A differenza dei prodotti analoghi dei concorrenti, il prodotto Dr.Web rende possibile il controllo antispam. Il modulo antispam, efficace e compatto, non richiede di essere istruito e permette di impostare azioni diverse per ciascuna categoria dello spam prevista dal programma, nonché di creare liste d'indirizzi email black and white.
- La tecnologia di rilevamento del malware sconosciuto (Origins Tracing) che permette di controllare anche archivi del formato sconosciuto distingue il prodotto Dr.Web dai suoi concorrenti.

### **Link utili**

Descrizione: <http://products.drweb.com/gateway/qbik>

## ► Dr.Web Mobile Security Suite

La protezione dei dispositivi mobili

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

	Dr.Web per il sistema operativo Symbian	Dr.Web per Windows Mobile	Dr.Web per Android
Elementi della protezione	Antivirus + Antispam	Antivirus + Antispam	Protezione integrata
Protezione centralizzata come parte di Dr.Web Enterprise Security Suite	-	+	+
Sistemi operativi supportati	S60, Symbian 9	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5	Android OS 4.0-5.0. Per il firewall Android 4.0 e superiori
<b>Funzionalità principali</b>			
Controllo in tempo reale ("al volo")	+	+	+
Controllo dei file ricevuti tramite la connessione GPRS/ Infrared/ Bluetooth/ Wi-Fi/ USB o durante la sincronizzazione con il PC	+	+	+
Due tipi di controllo: completo e a scelta	+	+	+
Possibile attivare/ disattivare il controllo continuo della scheda di memoria	+	+	+
Scansione a richiesta del sistema di file o dei singoli file e cartelle	+	+	+
Verifica dei file compressi in archivi dei formati ZIP, SIS, CAB, RAR	+	+	+
Liste nere e bianche delle telefonate e SMS entranti	+	+	+
Rimozione dei file infetti	+	+	+
I file sospetti vengono spostati in quarantena	+	+	+

I file possono essere ripristinati dalla quarantena	+	+	+
Aggiornamenti via Internet: <ul style="list-style-type: none"> <li>■ mediante il protocollo HTTP per mezzo del modulo GPRS incorporato;</li> <li>■ mediante le connessioni Infrared/Bluetooth/ Wi-Fi/ USB;</li> <li>■ tramite la sincronizzazione con il computer che ha l'accesso a Internet, mediante la connessione ActiveSync</li> </ul>	+	+	+
Rapporti dettagliati sulla scansione del sistema	+	+	+

## Licenze di Dr.Web Mobile Security Suite

Le licenze di Dr.Web Mobile Security Suite si acquistano secondo il numero dei dispositivi mobili da proteggere.

### Varianti di licenze

Dr.Web per Windows Mobile	Dr.Web per il sistema operativo Symbian	Dr.Web per Android
■ Antivirus + Antispam + Pannello di Controllo	■ Antivirus + Antispam	■ Protezione integrata + Pannello di Controllo

I prodotti Dr.Web per i dispositivi mobili sono anche disponibili nei pacchetti economici Dr.Web destinati alle piccole e medie aziende.

### Offerta speciale

La licenza gratuita di Dr.Web Mobile Security Suite viene concessa agli utenti registrati di Dr.Web Security Space e di Dr.Web Antivirus.

#### **Link utili**

Descrizione: <http://products.drweb.com/mobile/biz>

## Dr.Web Retail Security Suite

Prodotti per la vendita al minuto



Dr.Web Security Space



Antivirus Dr.Web



Pacchetto "Impresa Piccola"  
5 indirizzi di email / 1 anno

### 🔗 Link utili

Promemoria per venditore di prodotti al dettaglio:

[https://st.drweb.com/static/new-www/files/booklets/pamyatka\\_site\\_a5/Pamyatka\\_en.pdf](https://st.drweb.com/static/new-www/files/booklets/pamyatka_site_a5/Pamyatka_en.pdf)

## Pacchetti Dr.Web

I completi Dr.Web comprendono dei prodotti adatti per la protezione di tutti gli oggetti informatici.

**IMPORTANTE!** Nessuno sconto viene concesso per i pacchetti, neanche lo sconto per il rinnovo. Per rinnovare la licenza di un pacchetto, bisogna acquistare una licenza nuova del prezzo intero. Lo sconto sul rinnovo viene concesso solo se l'utente passa da un pacchetto ai prodotti separati Dr.Web.

### ► Pacchetto Dr.Web "Universale"

La protezione di tipo "Enterprise" è offerta a prezzi agevolati per le piccole e medie aziende.

Le piccole e medie aziende spesso non possono destinare una cospicua somma di denaro per la protezione informatica integrata. Offerto a prezzi agevolati, il pacchetto Dr.Web "Universale" è destinato alle aziende con un numero di computer da 5 a 50.

Prodotto	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mail Security Suite	Dr.Web Gateway Security Suite	Dr.Web Mobile Security Suite
Oggetti da proteggere	Workstation	Server	Utenti di posta elettronica	Utenti di gateway Internet e mail gateway	Dispositivi mobili
Licenza	Protezione integrata	Antivirus	Antivirus + Antispam	Antivirus	Antivirus
Allestimento	Da 5 a 50 workstation	1 server	Equivalente al numero delle workstation	Equivalente al numero delle workstation (a partire da 25)	Equivalente al numero delle workstation

### 🔗 Link utili

Pacchetti Dr.Web: <http://products.drweb.com/bundles/universal>

## ► Pacchetto Dr.Web per le scuole

Oggetti da proteggere	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mobile Security Suite
Licenza	Protezione integrata + Pannello di Controllo	Antivirus	
Allestimento	10 – 200 workstation	1 – 8 server	10 – 200 dispositivi mobili

## Utilità di disinfezione Dr.Web

Le utilità di disinfezione Dr.Web consentono la diagnostica e la disinfezione d'urgenza se necessaria. Esse non garantiscono la protezione continua del computer.

## ► Dr.Web CureNet!

**Quest'utilità serve per la disinfezione centralizzata delle reti locali di ogni livello, anche se vi è già stato installato l'antivirus di un altro produttore.**

Utenti potenziali	Imprese piccole, medie, grandi e maggiori, nelle cui reti locali è già stato installato l'antivirus di un altro produttore.
Obiettivi raggiungibili	<ul style="list-style-type: none"> <li>■ Disinfettare in modo centralizzato e remoto le workstation e i server Windows.</li> <li>■ Valutare la qualità della protezione antivirale fornita da un altro produttore.</li> </ul>
Caratteristiche dell'utilità	<ul style="list-style-type: none"> <li>■ Non è necessario rimuovere l'antivirus dell'altro produttore prima di controllare e disinfettare il computer.</li> <li>■ Non c'è bisogno di avere un server o installare ancora altro software.</li> <li>■ L'utilità si può usare nelle reti che sono completamente isolate da Internet.</li> <li>■ Il wizard Dr.Web CureNet! può essere avviato da qualsiasi supporto removibile, tra cui anche una chiave USB.</li> </ul>
Descrizione del prodotto	<a href="http://curenet.drweb.com/">http://curenet.drweb.com/</a>
Sistemi operativi supportati	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 (architettura a 32 e a 64 bit).
Che cos'è "Il mio Dr.Web CureNet!"?	È l'Area personale in cui si trova il collegamento individuale per scaricare gli aggiornamenti della distribuzione durante tutto il periodo di validità della licenza. Tramite l'Area personale si può anche mettersi in contatto con il supporto tecnico, spedire un file sospetto per essere analizzato, usufruire di altri servizi.
Licenze	Le licenze dell'utility vengono concesse per numero di postazioni (almeno 5) per 1, 2 e 3 anni di utilizzo.
Versione demo	La funzione di disinfezione non è disponibile nella versione demo.

<b>Requisiti di sistema</b>	<p><b>Wizard</b></p> <ul style="list-style-type: none"> <li>■ Un PC 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 (architettura a 32 e a 64 bit).</li> <li>■ RAM libera: almeno 360 MB.</li> <li>■ Spazio libero su disco rigido: almeno 200 MB.</li> <li>■ Connessione con tutte le postazioni da scansione attraverso il.</li> <li>■ Accesso ad Internet: per l'aggiornamento dei database dei virus e dei componenti di Dr.Web CureNet!</li> </ul> <p><b>Scanner</b></p> <ul style="list-style-type: none"> <li>■ Un PC MS Windows XP Professional e versioni successive, ad eccezione di Windows® Server 2003 x64 Edition e di Windows® XP Professional SP2 x64 Edition.</li> <li>■ RAM libera: almeno 360 MB.</li> <li>■ Spazio libero su disco rigido: almeno 200 MB.</li> </ul>
-----------------------------	--

## ► **Dr.Web CureIt!**

**Quest'utilità serve per la disinfezione d'urgenza dei PC gestiti da Windows, anche se vi è già stato installato l'antivirus di un altro produttore.**

<b>Utenti potenziali</b>	Piccole e medie imprese sui computer e server di quali ci è già stato installato l'antivirus di un altro produttore.
<b>Obiettivi raggiungibili</b>	<ul style="list-style-type: none"> <li>■ Disinfettare immediatamente le workstation e i server Windows.</li> <li>■ Valutare la qualità della protezione antivirale fornita da un altro produttore.</li> </ul>
<b>Caratteristiche dell'utilità</b>	<ul style="list-style-type: none"> <li>■ Non è necessario installarla, l'utilità non entra in conflitto con nessun antivirus, dunque per il tempo della scansione non è richiesto di disattivare l'antivirus di un altro produttore installato sul computer.</li> <li>■ Autodifesa incrementata e regime potenziato per reagire efficacemente ai Trojan.Winlock.</li> <li>■ Aggiornamenti una o più volte l'ora.</li> <li>■ L'utilità può essere avviata da qualsiasi supporto removibile, tra cui anche una chiave USB.</li> </ul>
<b>Descrizione del prodotto</b>	<a href="http://products.drweb.com/cureit">http://products.drweb.com/cureit</a>
<b>Sistemi operativi supportati</b>	MS Windows 8/7/Vista/XP/2000/Server 2012/2008/2003 (a 32 e 64 bit).
<b>Licenze</b>	L'utility viene concessa in licenza per 12, 24 e 36 mesi.
<b>Particolarità di licenze</b>	L'utilità è gratuita per curare il proprio PC di casa.
<b>Versione demo</b>	Non è disponibile.

## Soluzioni

Dr.Web Security Suite per UNIX Appliance è un gruppo di soluzioni a modulo che possono integrarsi con i complessi di dispositivi e programmi a base dei sistemi operativi UNIX (Linux / FreeBSD / Solaris (x86)).

Le soluzioni agiscono come il gateway Internet aziendale – un server proxy usato per l'accesso a Internet di utenti della rete interna.

	<b>Dr.Web Mail Security Suite per UNIX Appliance</b>	<b>Dr.Web Gateway Security Suite per UNIX Appliance</b>
<b>Funzionalità principale</b>	Filtrazione dei messaggi email alla ricerca di virus e spam	Filtrazione del traffico HTTP e FTP alla ricerca di virus
<b>Varianti di licenze</b>	Antivirus Antivirus + Antispam	Antivirus

### Tipi di licenze

- Licenza secondo il numero degli utenti protetti (illimitato).
- Licenza per un server – si può controllare la quantità illimitata della posta / del traffico su un server fino a 3.000 utenti protetti.

### Licenze dell'SDK

L'SDK è distribuito gratuitamente come parte del prodotto. Gli sviluppatori esterni possono sviluppare e distribuire i plugin in base all'SDK senza scopo di lucro. Per ricavare profitto dalla distribuzione di tali plugin, si dovrà superare il processo di certificazione.

## ▶ Dr.Web ATM Shield

Protezione antivirus centralizzata dei sistemi embedded (sportelli automatici, terminali POS, chioschi elettronici)

Potenziati utenti: banche (sportelli automatici), reti di supermercati (terminali POS, chioschi elettronici), nonché aziende che gestiscono processi di produzione (stazioni di servizio, stabilimenti ecc.).

### **Link utili**

Descrizione: [http://solutions.drweb.com/atm\\_shield](http://solutions.drweb.com/atm_shield)

### **Vantaggi**

- facile integrazione in una rete dei bancomat e dei dispositivi POS, di conseguenza, è necessario meno tempo per la manutenzione;
- è in grado di funzionare sui computer con una piattaforma hardware poco potente (512 MB) che sono in funzione per un lungo tempo senza possibilità di riavvio, cioè in modalità 24/7;
- gestione centralizzata di ogni componente di protezione antivirus dei sistemi embedded;
- la soluzione comprende i componenti che consentono di proteggere il sistema contro i programmi malevoli sconosciuti (non ancora esaminati dal laboratorio antivirus) e contro le azioni non autorizzate del personale addetto alla manutenzione;
- facile scalabilità che consente di utilizzare la soluzione nelle reti con un numero illimitato di host (grazie alla struttura gerarchica della rete antivirus);
- funziona nelle reti basate sullo stack di protocolli TCP/IP, IPX, sul NetBIOS;

- possibilità di scegliere il tipo di DBMS del server di protezione;
- trasmissione di dati di un volume minimo grazie a un apposito protocollo di scambio di informazioni che supporta la compressione di dati trasmessi tra i client e il server;
- possibilità di cifrare i dati trasmessi tra diversi componenti del sistema;
- controllo dello stato di ogni host protetto della rete;
- le informazioni statistiche sui virus vengono raccolte in maniera centralizzata;
- backup di dati critici del server di protezione della rete;
- trasparenza del funzionamento – un log di verifica delle azioni degli amministratori consente di tenere traccia di tutte le azioni di installazione e di configurazione eseguite nel sistema.

**ATTENZIONE!** Siccome l'utilizzo di strumenti antivirus sui dispositivi embedded ha qualche particolarità, si prega di consigliare ai clienti, prima di utilizzare Dr.Web ATM Shield, di studiare il manuale dell'amministratore (disponibile nella Procedura di download guidata dopo l'invio di una richiesta della versione demo) e di seguire un [corso di formazione](#) su questo prodotto.

## Licenze

- Vengono concesse per numero di dispositivi embedded da proteggere.
- La licenza del Pannello di controllo di Dr.Web ATM Shield è gratuita.

## Demo

Per ottenere una licenza di prova, è necessario compilare un questionario sulla pagina [http://download.drweb.com/demoreq/atm\\_shield](http://download.drweb.com/demoreq/atm_shield) indicando il numero di dispositivi da proteggere e il sistema operativo in uso (preferibile).

**ATTENZIONE!** Se sui dispositivi embedded del cliente si usano i sistemi operativi del tipo Embedded (MS Windows Embedded 7, MS Windows Embedded 8 ecc.), si prega di avvertirlo che tali sistemi operativi sono diversi dai normali sistemi operativi dato che vengono assemblati secondo il tipo dell'apparecchiatura e quindi in essi potrebbero mancare alcuni componenti potenzialmente necessari per far funzionare la protezione antivirus. Pertanto, il dispositivo da proteggere (come un'immagine) dovrebbe essere provato dal reparto sviluppo della società Doctor Web e in seguito al test Doctor Web potrebbe consigliare di installare i componenti mancanti.

## Link utili

Strumenti di marketing per i partner: [https://pa.drweb.com/products/atm\\_shield](https://pa.drweb.com/products/atm_shield)

## Web service

**Software as a Service (SaaS)** è un modello di distribuzione nel quale le applicazioni sono erogate da remoto da un provider esterno all'azienda utente. È ampiamente diffuso fuori dalla Russia.

Questo modello non era usato nel settore antivirus russo prima del 2007. La causa era la pura assenza delle soluzioni tecnologiche russe adatte per questo modello. La situazione è cambiata nel maggio del 2007 quando l'azienda russa Doctor Web S.r.l. ha lanciato il suo web service **Dr.Web AV-Desk**. Sul mercato di servizi IT russo si è apparso un nuovo segmento – servizi di protezione antivirus. Il primo fra essi è stato il servizio "Antivirus Dr.Web".

### ► Web service Dr.Web AV-Desk



<p><b>Che cos'è Dr.Web AV-Desk?</b></p>	<p><b>Dr.Web AV-Desk è un service web</b> che fornisce un insieme di servizi in linea della protezione informatica PC e server al numero illimitato di clienti – utenti privati e aziende.</p> <p><b>Dr.Web AV-Desk è un software</b> che permette di gestire in modo centralizzato la fornitura del servizio "Antivirus Dr.Web".</p> <p><b>Dr.Web AV-Desk è il modello di business VAD</b> con il quale diventa possibile attirare nuovi clienti e incrementare i redditi.</p>
<p><b>A chi è destinato Dr.Web AV-Desk?</b></p>	<p>Agli Internet provider e qualunque azienda che si occupa di tecnologie dell'informazione.</p>
<p><b>A chi è destinato il servizio "Antivirus Dr.Web"?</b></p>	<p>Alle persone private e giuridiche – clienti dei fornitori del servizio.</p>
<p><b>Che servizi può fornire il provider usando Dr.Web AV-Desk?</b></p>	<p>I servizi della protezione informatica dei PC clienti contro i virus, lo spam e diversi programmi malevoli. Tali servizi sono forniti a un utente abbonato per un periodo desiderato. L'utente può usare le funzioni protettive del software Dr.Web pagando il canone d'abbonamento.</p>
<p><b>Funzionalità del software Dr.Web AV-Desk</b></p>	<p>Dr.Web AV-Desk è un insieme di software che permette ai fornitori di gestire in modo centralizzato i servizi della protezione informatica dei PC forniti ai loro clienti.</p>
<p><b>Licenze di Dr.Web AV-Desk</b></p>	<p>Il service web Dr.Web AV-Desk è messo a disposizione del fornitore di servizi gratuitamente. A sua volta, il servizio "Antivirus Dr.Web" prevede l'acquisto di licenze secondo il numero degli utenti abbonati nel periodo di riferimento (un mese) con l'abbonamento ancora valido.</p>

## Come funziona?

Fornitore del servizio	Clienti del servizio
<ul style="list-style-type: none"> <li>■ Organizza l'abbonamento al servizio "Antivirus Dr.Web" tramite il Controllo dell'abbonamento.</li> <li>■ Provvede che i clienti del servizio ricevano gli aggiornamenti dei database virus e dei moduli software Dr.Web.</li> <li>■ Provvede il supporto tecnico (è opzionale).</li> <li>■ Rintraccia lo stato della rete antivirale e raccoglie i dati statistici delle infezioni virus.</li> <li>■ Fornisce i servizi supplementari.</li> <li>■ Riscuote il canone d'abbonamento dai clienti abbonati al servizio.</li> </ul>	<ul style="list-style-type: none"> <li>■ Si abbonano al servizio tramite il Controllo dell'abbonamento.</li> <li>■ Installano il software Dr.Web.</li> <li>■ Gestiscono i parametri del loro abbonamento.</li> <li>■ Pagano il canone d'abbonamento al fornitore del servizio.</li> </ul>

Dr.Web AV-Desk è un modello di business a molte varianti. Un Internet provider o qualunque azienda che si occupa di tecnologie dell'informazione può diventare fornitore del servizio "Antivirus Dr.Web".

	Rivenditore del servizio "Antivirus Dr.Web"	Fornitore del servizio "Antivirus Dr.Web"	Aggregatore del service Dr.Web AV-Desk
<b>Business principale</b>	L'impresa attua l'abbonamento degli utenti finali al servizio "Antivirus Dr.Web" tramite il Controllo dell'abbonamento integrato nel suo sito d'Internet.	L'impresa implementa il service Dr.Web AV-Desk e fornisce il servizio "Antivirus Dr.Web" agli utenti finali.	L'impresa possiede dei server su cui implementa il service Dr.Web AV-Desk, crea la propria rete di rivenditori del servizio cui concede in sottolicensing i Controlli dell'abbonamento senza il diritto di vendere il servizio agli utenti finali.

I partner di Doctor Web S.r.l. possono richiedere l'informazione dettagliata su Dr.Web AV-Desk e sul servizio "Antivirus Dr.Web".

### Link utili

Nuovo esame del corso di formazione DWCERT-004 Dr.Web AV-Desk v.6:

<https://pa.drweb.com/training/engineers/>

Nuovo esame del corso di formazione DWCERT-010-3 Servizio "Antivirus Dr.Web":

<https://pa.drweb.com/training/courses/tech/>

## Politica di sconti

I coefficienti di sconto si applicano al prezzo di una licenza valida per un anno (secondo il listino prezzi).

Se l'utente ha diritto a più tipi di sconti, essi non vengono sommati, ma viene concesso all'utente lo sconto più grande (a eccezione di fornitori di servizi Internet).

Gli sconti sono applicati solamente alle soluzioni presenti nel listino prezzi. Gli sconti sulle soluzioni che non sono nel listino prezzi devono essere concordati con Doctor Web S.r.l.

### Sconti per quantità di prodotti di Dr.Web Enterprise Security Suite

Gli sconti concessi per numero di prodotti acquistati (dei tipi di oggetti da proteggere) sono calcolati sulla somma dei prezzi delle licenze base e delle licenze degli elementi complementari – separatamente per ogni prodotto. Questi sconti sono conteggiati automaticamente dalla calcolatrice.

Numero dei prodotti acquistati	Sconto	Rabatt
4		30%
3		25%
2		20%

**Eccezione:** gli sconti non sono previsti per il prodotto Dr.Web Mobile Security.

### Limitazioni

Gli sconti non vengono applicati se:

- il numero dei server costituisce meno del 10% del numero di workstation, degli utenti di posta elettronica o di gateway;
- il numero degli utenti di posta elettronica o di gateway è minore del numero di workstation;
- il numero degli utenti di gateway è minore del numero degli utenti di posta elettronica e viceversa.

### Tabella di sconti

Tipo di cliente	Titolo per lo sconto	Licenza nuova			Rinnovo della licenza			Migrazione		
		1 anno	2 anni	3 anni	1 anno	2 anni	3 anni	1 anno	2 anni	3 anni
Categorie senza agevolazione	Per avere uno sconto sul rinnovo si deve presentare il file chiave oppure il numero seriale Dr.Web di un prodotto simile Dr.Web con la durata della licenza di almeno 6 mesi									
	Per avere uno sconto sulla migrazione si deve presentare l'originale della licenza / il file chiave / la lettera che conferma l'acquisto della versione elettronica dell'antivirus di un altro produttore	-	1,6	2,17	0,6	1,17	1,72	0,5	1	1,5
Istituzioni scolastiche e universitarie, biblioteche, musei, istituzioni di sanità pubblica	Copia della licenza d'istruzione/ del certificato di registrazione / della licenza del Ministero di sanità pubblica e questionario riempito	0,5	0,85	1,2	0,35	0,7	1,05			

## Condizioni del rinnovo

1. Applicando gli sconti, si può rinnovare sia una licenza Dr.Web ancora valida, sia una già scaduta. Non importa da quanto tempo sia scaduta.
2. Con l'applicazione degli sconti si può rinnovare una licenza del prodotto o di una soluzione analoga Dr.Web. La durata della licenza deve essere almeno 6 mesi.
3. Lo sconto sul rinnovo viene concesso se si acquista la licenza del prodotto o di una soluzione analoga Dr.Web della durata di uno, due o tre anni.
4. La licenza rinnovo scontata viene concessa per il numero di oggetti da proteggere che non eccede il numero specificato nella licenza precedente (quella da rinnovare).
5. I titoli per ricevere lo sconto sul rinnovo sono il file chiave o il numero seriale Dr.Web che possono essere rinnovati una sola volta.
6. Per ricevere lo sconto sul rinnovo, l'utente deve presentare al venditore il numero seriale o il file chiave (anche OEM).

## “Passa al verde!”

È un piano di migrazione agevolata verso Dr.Web per gli utenti che usano antivirus di altri produttori.

1. Quest'offerta speciale vale solo per i prodotti Dr.Web. La migrazione agevolata non è prevista per i pacchetti, le utilità, le combinazioni di dispositivi e programmi e le soluzioni già Dr.Web.
2. Lo sconto non è concesso ai privati. Lo sconto è offerto solo alle aziende e agli enti i quali ne possono beneficiare solo una volta.
3. Lo sconto sulla migrazione non è concesso agli utenti di licenze OEM.
4. Nel caso di migrazione verso Dr.Web la licenza di un anno viene scontata dal 50%. Lo sconto sulle licenze di due e tre anni è calcolato in base al rispettivo coefficiente 1 o 1,5 il quale viene moltiplicato per il prezzo della licenza Dr.Web annuale.
5. Lo sconto sulla migrazione è concesso solamente sui prodotti analoghi Dr.Web (secondo il tipo e il numero di oggetti da proteggere).
6. Per ricevere lo sconto sulla migrazione, l'utente deve presentare l'originale della licenza, il file chiave oppure la lettera che conferma l'acquisto della versione elettronica dell'antivirus di un altro produttore con i dati di registrazione.
7. Lo sconto è concesso agli utenti delle licenze ancora valide o già scadute a condizione che siano passati al massimo 30 giorni dalla scadenza al momento in cui il cliente si è rivolto a un partner di Doctor Web S.r.l.
8. Se al momento della migrazione la licenza dell'antivirus di un altro produttore è ancora valida, il tempo rimasto viene aggiunto gratuitamente alla durata della nuova licenza Dr.Web.
9. In seguito le licenze di migrazione sono rinnovate con il solito sconto concesso sui rinnovi.
10. Gli sconti sulla migrazione non vengono sommati con nessun altro sconto.

## Condizioni generali di vendita

1. I partner devono vendere i software Dr.Web agli utenti finali attenendosi rigorosamente all'allestimento previsto e ai prezzi consigliati fissati nel listino prezzi.
2. Per tutti i prodotti Dr.Web di allestimento standard, i prezzi fissati nel listino già comprendono i costi degli aggiornamenti dei software e dei database virus e i costi del supporto tecnico di base accessibile tramite un modulo web sulla pagina <http://support.drweb.com>.
3. Se si ordinano le licenze in confezione con il logo Dr.Web, il loro prezzo si aumenta per il prezzo del pacchetto media (tranne i prodotti forniti come «Confezioni»).
4. Se all'acquirente occorre una soluzione per proteggere più oggetti di quanti sono specificati nel listino prezzi, il partner deve richiedere i rispettivi prezzi a Doctor Web S.r.l. e fornire tramite il modulo web sulla pagina <https://pa.drweb.com/support> le seguenti informazioni dell'acquirente:
  - il nome dell'azienda;
  - l'indirizzo;
  - e-mail;
  - il numero di telefono dell'impiegato responsabile per la protezione antivirus;
  - i contatti del servizio di supporto tecnico del partner.

Nel caso della vendita di tali soluzioni, lo sconto di qualsiasi tipo viene concesso all'utente finale solo se acconsentito da Doctor Web S.r.l.

5. I prezzi per le soluzioni non specificate nel listino prezzi sono determinati dal contratto di licenza che viene stipulato da Doctor Web S.r.l. con il fornitore che fornisce tali soluzioni direttamente agli utenti finali.

### **Link utili**

Modulo di richiesta dei prezzi dei prodotti antivirus Doctor Web:  
<https://pa.drweb.com/support/price1/>

# Acquisto supplementare in caso di Dr.Web Enterprise Security Suite

## Regole generali

1. L'acquisto supplementare connesso a una licenza non scaduta (o ampliamento della licenza) può essere dei seguenti tipi:
    - **qualitativo** – se alla licenza attuale si aggiungono nuovi componenti di protezione, mentre i prodotti inclusi nella licenza non cambiano.
    - **quantitativo** – se aumenta il numero di oggetti protetti rispetto alla licenza attuale senza cambiamento dei prodotti inclusi nella licenza attuale.
    - **acquisto supplementare dei prodotti** – se alla licenza attuale si aggiungono nuovi prodotti.
- Inoltre, un acquisto supplementare può essere una combinazione dei tipi descritti sopra.
2. L'acquisto supplementare è possibile se la durata della licenza è al minimo 3 mesi e al massimo 33 mesi.
  3. Il tempo residuo di validità della licenza si calcola sulla base del numero di mesi rimanenti fino alla scadenza della licenza precedente (in questo caso un mese incompleto deve essere arrotondato a 1 mese).
  4. L'acquisto supplementare è possibile solo se la licenza non è ancora scaduta e fino alla scadenza rimangono almeno 3 mesi – altrimenti è necessario effettuare un acquisto supplementare insieme al rinnovo.
  5. Nel codice della licenza nuova, il tipo di licenza è C (acquisto supplementare).
  6. La licenza di acquisto supplementare si attiva automaticamente al momento di generazione.
  7. La licenza precedente si blocca un giorno dopo la registrazione della licenza di acquisto supplementare, e non può essere rinnovata. Per effettuare un rinnovo, il cliente deve presentare la licenza di acquisto supplementare.

## Acquisto supplementare più rinnovo

1. L'acquisto supplementare con il rinnovo è possibile se la licenza è ancora valida o già scaduta.
2. Se una licenza ancora valida viene ampliata da un acquisto supplementare e rinnovata, le durate della licenza precedente (non scaduta) e di quella nuova (acquisto supplementare più rinnovo) si sommano.
3. Nel codice della licenza nuova, il tipo di licenza è D (acquisto supplementare + rinnovo).
4. La licenza di acquisto supplementare si attiva automaticamente al momento di generazione.
5. La licenza precedente (quella rinnovata) si blocca un giorno dopo la registrazione della licenza nuova (acquisto supplementare più rinnovo), e non può essere rinnovata. Per effettuare un rinnovo, il cliente deve presentare la licenza di acquisto supplementare.
6. In caso di simultaneo rinnovo e acquisto supplementare, il prezzo delle licenze DI ACQUISTO SUPPLEMENTARE si calcola sulla base del prezzo dell'intervallo a cui appartiene la quantità totale delle licenze acquistate (licenze rinnovate + licenze di acquisto supplementare). Il prezzo delle licenze RINNOVATE si calcola sulla base del prezzo dell'intervallo a cui appartiene la quantità totale delle licenze RINNOVATE.

## Regole per calcolare il prezzo delle licenze di acquisto supplementare

**I. Acquisto supplementare qualitativo (alla licenza attuale si aggiungono componenti addizionali, mentre il numero di oggetti protetti e i prodotti non cambiano).**

1. Se il cliente vuole **migrare dalla licenza Antivirus verso Protezione completa del prodotto Dr.Web Desktop Security Suite**, si applica un sovrapprezzo del 20% sul prezzo della licenza Antivirus diviso proporzionalmente per il numero dei mesi rimanenti fino alla scadenza.

### Esempio

La nuova licenza Antivirus per 90 PC costa 1 368,90 Euro. Due mesi dopo aver cominciato a usarla, il cliente vuole migrare alla Protezione completa.

$1\ 368,90 \text{ Euro} \div 12 \text{ mesi} \times 0,2 \text{ (sovrapprezzo del 20\%)} \times 10 \text{ mesi} = 228,15 \text{ Euro}$  (supplemento da pagare per la migrazione alla Protezione completa).

In totale, la licenza costa **1 597,05 Euro**.

2. Se il cliente effettua un acquisto supplementare dell'**Antispam**, componente dei prodotti Dr.Web Mail Security Suite o Dr.Web Gateway Security Suite, si applica un sovrapprezzo del 40% sull'importo pagato per la licenza Antivirus o Antivirus + SMTP proxy.

### Esempio

Il cliente ha acquistato per 1 101,60 Euro una licenza Antivirus per la protezione di 90 utenti della posta elettronica e due mesi dopo ha deciso di aggiungere l'Antispam.

$1\ 101,60 \text{ Euro} \div 12 \text{ mesi} \times 0,4 \times 10 \text{ mesi} = 367,20 \text{ Euro}$  (supplemento da pagare per l'acquisto dell'Antispam).

In totale, la licenza costa **1 468,80 Euro**.

3. Se il cliente vuole aggiungere il componente **SMTP proxy**, si applica un sovrapprezzo del 20% sul prezzo della licenza Antivirus o Antivirus + Antispam.

## Tabella riassuntiva dei sovrapprezzi applicati agli acquisti supplementari qualitativi senza aumento del numero di oggetti protetti

Prodotto	Licenza attuale	Licenza nuova	Sovrapprezzo
Dr.Web Desktop Security Suite	Antivirus	Protezione completa	20%
Dr.Web Mail Security Suite o Dr.Web Gateway Security Suite	Antivirus	+ Antispam	40%
	Antivirus + SMTP proxy		
	Antivirus	+ SMTP proxy	20%
	Antivirus + Antispam		

## II. Acquisto supplementare quantitativo (aumento del numero di oggetti protetti)

Il prezzo delle licenze di acquisto supplementare si calcola in base al listino prezzi valido selezionando l'intervallo a cui appartiene la quantità totale di oggetti protetti **senza alcuno sconto**.

### III. Acquisto supplementare dei prodotti (aggiunzione dei prodotti alla licenza)

Il prezzo delle licenze di acquisto supplementare si calcola in base al listino prezzi valido **senza sconto per quantità di prodotti**.

#### Prodotti per l'impresa per cui non è previsto un acquisto supplementare

- Prodotto Dr.Web "Piccola impresa" in scatola.
- Pacchetto licenze "Dr.Web Universale" e Dr.Web per le scuole.

Per ampliare una licenza di questi prodotti, il cliente deve migrare verso Dr.Web Enterprise Security Suite secondo le regole di acquisto supplementare più rinnovo.

## Codici dei prodotti, dei pacchetti, delle utilità e delle combinazioni di dispositivi e programmi Dr.Web

### Regole per la formazione dei codici

1. Ogni codice consiste di 5 gruppi.
2. Ogni gruppo è separato da un altro gruppo con un trattino.
3. Il codice di una licenza della categoria "Prodotti" viene formato separatamente per ogni prodotto Dr.Web commerciale (veda la sezione "Linea dei prodotti Dr.Web Security Suite").
4. I codici delle combinazioni di dispositivi e programmi consistono di due codici:
  - codice del dispositivo,
  - codice della licenza.
5. I codici dei prodotti confezionati, delle schede da grattare e dell'hardware dell'insieme di dispositivi e programmi Dr.Web Office Shield sono specificati nel listino prezzi e sono fissi.
6. Due termini sono indicati nel codice di una licenza acquistata in supplemento: la durata generale della licenza acquistata in supplemento e – dopo il doppio punto – la durata restante della chiave allegata (quella già in vigore).
7. Due termini sono indicati nel codice di una licenza nel caso dell'acquisto supplementare più il rinnovo: la durata generale della licenza acquistata in supplemento e rinnovata e – dopo il doppio punto – la durata restante della chiave allegata (quella da rinnovare).
8. Due numeri degli oggetti da proteggere sono indicati nel codice di una licenza acquistata in supplemento: il numero cumulativo delle licenze, incluse quelle acquistate in supplemento e – dopo il doppio punto – il numero degli oggetti della licenza già in vigore (allegata).
9. Due numeri degli oggetti da proteggere sono indicati nel codice di una licenza nel caso dell'acquisto supplementare più il rinnovo: il numero cumulativo delle licenze, incluse quelle acquistate in supplemento e rinnovate – dopo il doppio punto – il numero degli oggetti della licenza già in vigore (quella da rinnovare).

## Tabella riassuntiva dei codici

1° gruppo			2° gruppo		3° gruppo	4° gruppo	5° gruppo	
Allestimento	Categoria del prodotto	Oggetti da proteggere	Licenza base	Elementi complementari	Durata della licenza	Numero di oggetti da proteggere	Tipo di licenza	Agevolazione
<b>L</b> – un esemplare del software (prodotto) scaricato dal sito web	<b>B</b> – prodotto per le aziende <b>H</b> – prodotto per i privati	<b>G</b> – utenti di gateway	<b>A</b> – Antivirus	<b>A</b> – Antispam	<b>XXM</b> – dove XX è il numero di mesi	Qualsiasi numero	<b>A</b> – nuova licenza	<b>1</b> – istituzione scolastica o universitaria, biblioteca, museo, istituzione di sanità pubblica
<b>B</b> – un esemplare del software in confezione di cartone <b>A</b> – un esemplare del software in confezione di cartone promozionale	<b>X</b> – un esemplare del software consegnato insieme a Dr.Web Office Shield	<b>M</b> – dispositivi mobili	<b>B</b> – Protezione Integrata	<b>C</b> – Pannello di Controllo	<b>XXXD</b> – dove XXX è il numero di giorni	<b>UL</b> – numero illimitato (per una licenza illimitata)	<b>B</b> – rinnovo della licenza	<b>2</b> – promozione
							<b>C</b> – acquisto supplementare	<b>3</b> – senza agevolazioni
<b>C</b> – una scheda con la striscia da grattare	<b>Y</b> – utilità	<b>P</b> – utenti di posta elettronica	<b>K</b> – Katana	<b>K</b> – senza elementi complementari			<b>D</b> – rinnovo e acquisto supplementare	<b>4</b> – migrazione
<b>D</b> – un esemplare del software in confezione DVD	<b>Z</b> – pacchetto	<b>S</b> – server	<b>*</b> – licenze di più prodotti (solo per Pacchetti)	<b>R</b> – Crittografo			<b>R</b> – Rescue pack	<b>5</b> – licenza NFR per il partner
<b>K</b> – un esemplare del software in busta di licenza		<b>W</b> – workstation		<b>S</b> – SMTP proxy			<b>F</b> – licenza OEM	<b>6</b> – licenza NFR (demo) per il cliente
<b>M</b> – un esemplare del software sul disco marchiato (anche OEM)		<b>Z</b> – tutti gli oggetti					<b>G</b> – licenza di servizio	<b>7</b> – esigenze di marketing/formazione
<b>N</b> – un esemplare del software in pacchetto media certificato							<b>H</b> – senza supporto tecnico	<b>8</b> – beneficenza
<b>P</b> – un esemplare del software in pacchetto media per licenze OEM							<b>V</b> – cliente importante	<b>9</b> – divisione di una chiave
<b>Q</b> – vendite via SMS								<b>10</b> – fusione di più chiavi
								<b>11</b> – sostituzione della chiave

## Esempi

### Esempi dei codici licenze della categoria "Prodotti"

1.	Il cliente – un'istituzione scolastica richiede la protezione di 200 PC con il Pannello di Controllo, comprendente la Protezione Integrata + il Firewall + il Crittografo, della durata di 12 mesi, licenza elettronica. Il cliente acquista un programma Dr.Web per la prima volta.	LBW-BRC-12M-200-A1
2.	Il cliente – un'istituzione scolastica ha una licenza valida per di 200 PC con il Pannello di Controllo, comprendente la Protezione Integrata + il Firewall + il Crittografo, della durata di 12 mesi, licenza elettronica. Rimangono 6 mesi prima della scadenza della licenza. Il cliente desidera acquistare in supplemento la protezione per altri 10 PC.	LBW-BRC-6M:6M-210:200-C1
3.	Il cliente – un'istituzione scolastica ha una licenza specificata nel secondo esempio. Rimangono 7 mesi prima della scadenza della licenza. Il cliente desidera acquistare in supplemento la protezione per altri 10 PC e anche rinnovare la licenza per altri 2 anni.	LBW-BRC-31M:7M-210:200-D1

### Esempi dei codici licenze della categoria "Pacchetti"

1.	Il cliente richiede il pacchetto Dr.Web "Universale" per la protezione di 50 PC con il Pannello di Controllo, comprendente la Protezione Integrata + il Crittografo, la durata di 12 mesi, licenza elettronica.	LZZ-*CR-12M-50-A3
2.	Il cliente richiede il pacchetto Dr.Web "Universale" per la protezione di 50 PC con il Pannello di Controllo, comprendente la Protezione Integrata, la durata di 12 mesi, licenza elettronica.	LZZ-*C-12M-50-A3
3.	Il cliente – un'istituzione scolastica richiede la protezione di 100 PC.	LZZ-*C-12M-100-A1

### Esempi dei codici licenze della categoria "Utilità"

1.	Al cliente occorre disinfettare 100 PC durante 10 giorni. I computer sono uniti in una rete aziendale.	LYW-AC-10D-100-A3
2.	Al cliente occorre disinfettare 10 PC durante 30 giorni. I computer non sono uniti in network aziendale.	LYW-AK-30D-10-A3

### Esempi dei codici licenze della categoria "Combinazioni di dispositivi e programmi Dr.Web Office Shield"

Sono generati tanti codici, quante licenze dei prodotti Dr.Web sono acquistate.

1.	Il cliente – un'istituzione scolastica richiede la protezione di 25 utenti di posta elettronica (AB+AC+SMTP proxy) e di 50 utenti di gateway Internet.	LXP-AASC-12M-25-A1 LXG-AK-12M-50-A1
2.	Il cliente richiede la protezione integrata di 150 PC, di un server Windows, di 100 utenti di posta elettronica (solo l'antivirus) e di 50 utenti di gateway Internet.	LXW-BC-12M-150-A3 LXS-AC-12M-1-A3 LXP-AC-12M-100-A3 LXG-AC-12M-50-A3
3.	Il cliente ha la licenza specificata nel secondo esempio la quale scade in 7 mesi. Il cliente desidera acquistare in supplemento la protezione per altri 20 PC e anche rinnovare la licenza per 1 anno.	LXW-BC-19M:7M-170:150-D3 LXS-AC-19M-1-B3 LXP-AC-19M-100-B3 LXG-AK-19M-50-B3

### Esempi dei codici dei prodotti OEM

1.	Il partner acquista 500 schede OEM in pacchetti media.	PHW-B-6M-1-F3
2.	Il partner acquista 500 licenze OEM consegnate sui dischi.	MHW-B-6M-1-F3

## Contatti:

### Russia

#### Dr.Web S.r.l.

Russia, 125124, Mosca, via 3 Yamskogo Polya, tenuta 2, edificio 12A

Telefono: +7 (495) 789-45-87 (centralino)

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

[www.drweb.com](http://www.drweb.com) | [www.av-desk.com](http://www.av-desk.com) | [www.freedrweb.com](http://www.freedrweb.com)

### Germania

#### Doctor Web Deutschland GmbH

Deutschland, 63457 Hanau, Rodenbacher Chaussee 6

Telefono: +49 (6181) 9060-1210

Fax: +49 (6181) 9060-1212

[www.drweb-av.de](http://www.drweb-av.de)

### Kazakistan

#### TOO "Doctor Web – Tsentralnaya Asia"

Kazakistan, 050009, Almaty, via Shevchenko / angolo via Radostovtza, 165b/72g, ufficio 910

Telefono: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32

[www.drweb.kz](http://www.drweb.kz)

### Ucraina

#### Centro del supporto tecnico "Doctor Web"

Ucraina, 01601, Pushkinskaya, 27, office 6

Telefono / fax: +38 (044) 238 24 35

[www.drweb.ua](http://www.drweb.ua)

### Francia

#### Doctor Web France

333 b Avenue de Colmar, 67100 Strasbourg, France

Telefono: +33 (0) 3 90 40 40 20

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

[www.drweb.fr](http://www.drweb.fr)

### Giappone

#### Doctor Web Pacific, Inc.

NKF Kawasaki building 2F,

1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005, Japan

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

[www.drweb.co.jp](http://www.drweb.co.jp)

### Cina

#### Doctor Web Software Company (Tianjin), Ltd.

112, North software tower, № 80, 4th Avenue, TEDA, Tianjin, China

天津市经济技术开发区第四大街80号软件大厦北楼112

Tel: +86-022-59823480

Fax: +86-022-59823480

[www.drweb.com](http://www.drweb.com)