Hai qualcosa da proteggere?

Noi abbiamo Dr.WEB®

dal 1992

Sommario

L’azienda Dr.Web

L’azienda Doctor Web S.r.l. è un produttore russo di mezzi di sicurezza informatica molto conosciuto in Russia ed in diversi Paesi nel 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 in Russia che in altri Paesi.

Oggi Doctor Web è un’azienda che cresce velocemente e ottiene molti successi e che può essere considerata leader nel mercato dei mezzi di sicurezza informatica. Noi disp niamo 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. Di pari importanza è lo sviluppo di 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.

Avendo rinunciato alla vendita diretta agli utenti finali l’azienda detiene una rete distributiva tramite partner.

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 mostrati nel corso degli anni a Dr.Web. 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 di una propria tecnologia di rilevamento ed eliminazione. Abbiamo un nostro servizio di monitoraggio antivirus e un laboratorio analitico grazie al quale 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.

Oltre ai virus e ai 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 orignale pulito. Dr.Web tratta i file dell'utente con premura.

Disinfezione

- Dr.Web, a differenza di tutti gli altri programmi analoghi, opera con successo sul computer già infettato ed è invulnerabile ai virus.
- Dr.Web ha la percentuale più alta nell'industria antivirus relativamente alla disinfezione efficace nel caso di infezione attiva.
- Non è necessario disinfettare il computer prima di installare Dr.Web: grazie alle sue tecnologie uniche di elaborazione dei processi nella memoria e alle sue capacità superiori nella neutralizzazione dell'infezione attiva, Dr.Web può essere installato direttamente sul computer infetto.
- C'è una probabilità elevata che la scansione si avvii sul PC infetto – persino dal supporto rimovibile (quale una chiave USB) senza necessità di installazione.

Autodifesa

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

- Dr.Web SelfPROtect è stato realizzato come driver e funziona al livello più profondo del sistema operativo – il suo funzionamento può essere interrotto solo dal riavvio del sistema. Per questo i malware non possono minare l'autodifesa.
- Dr.Web SelfPROtect limita l'accesso dei malware alla rete, ai file e alle cartelle, ad alcuni rami del registro di sistema e ai supporti rimovibili agendo come driver del sistema operativo e protegge dai tentativi dei programmi anti-antivirus di interrompere il funzionamento di Dr.Web.
- Dr.Web SelfPROtect è del tutto autosufficiente e a differenza di altri prodotti rivali non modifica il nucleo di Windows. Determinate operazioni effettuate da altri programmi antivirus possono provocare gravi problemi nel funzionamento del sistema operativo stesso e aprono anche nuove strade ai malintenzionati, i quali potranno poi sfruttare le vulnerabilità del computer.

Capacità uniche del nucleo antivirus

- Verifica gli archivi di tutti i livelli gerarchici.
- Rileva con un grado elevato di precisione i malware compressi (anche se compressi in un modo sconosciuto a Dr.Web), li scompone e li analizza dettagliatamente ai fini di scoprire le minacce nascoste.
- Dr.Web è ineguagliabile nel rilevamento e nella neutralizzazione dei virus composti quali Shadow.based (Conficker), MaosBoot, Rustock.C, Sector.
- Le tecnologie intellettuali per la verifica della memoria consentono di bloccare i virus attivi prima che le loro copie appaiano sul disco rigido del computer, quindi diventa meno probabile che i malware sfruttino le vulnerabilità delle applicazioni installate o del sistema operativo.

- Rivela e neutralizza i virus che risiedono nella memoria operativa e non si manifestano mai nella forma di un singolo file (quali Slammer e CodeRed).

Protezione contro le minacce sconosciute

- FLY-CODE è una tecnologia unica che è in grado di decomprimere i file compressi in un modo sconosciuto a Dr.Web.
- L'Origins Tracing, la tecnologia unica della ricerca non basata sulle firme antivirali consente a Dr.Web di rilevare con un grado elevato di probabilità i malware che non sono ancora stati inseriti nel database virus.
- L'analizzatore euristico Dr.Web rileva efficacemente tutte le minacce diffuse stabilendo la loro classe in base all'esame fatto e alle loro proprietà caratteristiche.
- **Dr.Web Process Heuristic** protegge dai programmi malevoli nuovi che non possono essere rilevati con i tradizionali metodi di analisi basata sulle firme antivirali e di analisi euristica. Tali malware non sono ancora arrivati nel laboratorio antivirale e sono sconosciuti dal database dei virus Dr.Web al momento quando cercano di insediarsi nel sistema. Analizza il comportamento di un programma pericoloso e determina se è un programma nocivo, dopo di che esegue le azioni necessarie per neutralizzare la minaccia. La nuova tecnologia di protezione di dati da corruzione permette di minimizzare danni causati da azioni di un virus sconosciuto.
- **L'analisi integrata delle minacce pacchettate** rende più efficace il rilevamento delle minacce apparentemente nuove, conosciute dal database dei virus Dr.Web, ma nascoste tramite packer nuovi, e inoltre rende non necessaria l'aggiunzione di sempre nuovi record ai database dei virus. Grazie alla piccola dimensione dei database Dr.Web, non è necessario aumentare di continuo i requisiti di sistema dell'antivirus, inoltre gli aggiornamenti consumano poca banda, mentre la qualità di rilevamento e di cura è alta.

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 di 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 potrebbe 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 ad un 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 notifiche di un messaggio non 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 nostra tecnologia di creazione del database virus in base al linguaggio molto flessibile elaborato per 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), e ci sono persino virus creati usando utility di costruttori di 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 Dr.Web

- Numero minimo di firme antivirali.
- Il piccolo volume degli aggiornamenti.
- Una sola firma consente di riconoscere decine o centinaia, talvolta, 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 pur 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 minimo di 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 co pressi in archivi.

Dr.Web Enterprise Security Suite

Prodotti per l'impresa

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 in 5 gruppi per tipo di oggetto da proteggere.

Prodotto	Programmi
Dr.Web Desktop Security Suite 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 KATANA
	Dr.Web per Linux
	Dr.Web per macOS
	Dr.Web per MS DOS
	Dr.Web per OS/2
Dr.Web Server Security Suite Protezione dei file server e server di applicazioni (compresi terminal server e server virtuali)	Dr.Web per Windows server
	Dr.Web per Unix server
	Dr.Web per Novell NetWare server
	Dr.Web per macOS Server
Dr.Web Mail Security Suite Protezione della posta elettronica	Dr.Web per 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 Kerio mail server per Windows
	Dr.Web per Kerio mail server per Linux
	Dr.Web per Kerio mail server per macOS
Dr.Web Gateway Security Suite Protezione dei gateway	Dr.Web per Unix Internet Gateway
	Dr.Web per Kerio Internet Gateway
	Dr.Web per MIMEsweeper
	Dr.Web per Qbik WinGate
	Dr.Web per Microsoft ISA Server e Forefront TMG
Dr.Web Mobile Security Suite Protezione dei dispositivi mobili	Dr.Web per Android
	Dr.Web per BlackBerry

Licenza di Dr.Web Enterprise Security Suite

Le licenze dei prodotti vengono concesse separatamente per ciascun oggetto. Per la protezione di ciascun oggetto occorre scegliere una licenza base e, se necessario, i componenti addizionali.

Oggetti da proteggere	Sistemi operativi e piattaforme supportati	Licenza di base	Elementi complementari
Dr.Web Desktop Security Suite Workstation Client dei terminal server Client dei server virtuali Client dei sistemi incorporati	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bit). Windows 10/8/8.1/7/Vista SP2 (64 bit).	Protezione integrata	■ Pannello di controllo
		Antivirus	
	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (32 bit). Windows 10/8/8.1/7/Vista SP2 (64 bit).	KATANA	
	Linux glibc 2.7 e superiore macOS 10.7 e superiore	Antivirus	■ Pannello di controllo
	MS DOS* OS/2*		
Dr.Web Server Security Suite File server Server di applicazioni Terminal server Server virtuali	Windows Novell NetWare macOS Server UNIX (Samba)	Antivirus	■ Pannello di controllo
Dr.Web Mail Security Suite 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
Dr.Web Gateway Security Suite Utenti di gateway Internet	Kerio Internet Gateway UNIX Internet Gateway	Antivirus	■ Pannello di controllo
	MIMEsweeper Qbik WinGate		■ Antispam
Dr.Web Mobile Security Suite Dispositivi mobili	Android OS 4.0—7.1, Android TV 5.0+	Protezione completa	■ Pannello di controllo
	BlackBerry 10.3.2+	Protezione completa	

Universalità

In conformità con la soluzione selezionata dal cliente, viene creato il file della chiave Dr.Web singolo per la protezione di tutti gli oggetti richiesti. La chiave include i prodotti di programma Dr.Web di protezione di un oggetto per ogni sistema operativo e piattaforma supportata da Dr.Web.

Link utili

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

Pannello di controllo Dr.Web

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

Funzioni principali

- Gestione centralizzata di tutti gli elementi della protezione, esamina continuamente lo stato di tutte le unità protette della rete ed è possibile impostare la reazione automatica sugli incidenti virus.

Vantaggi

- Possibilità di proteggere in modo centralizzato tutti i nodi, dispositivi e servizi di una rete.
- Minimo costo complessivo in confronto ai programmi concorrenti, grazie alla possibilità di creare una rete con i server sia Windows che Unix, alla semplicità dell'installazione e all'affidabilità della protezione.
- L'installazione è possibile sia sui sistemi operativi a 32 bit che su quelli a 64 bit.
- Possibilità di installare il software agent immediatamente sulla macchina già infettata, e alta probabilità di guarigione.
- Minimo consumo delle risorse dei computer e dei server grazie alla compattezza del nucleo antivirus e all'utilizzo in esso delle tecnologie moderne.
- Amministrazione remota tramite un'interfaccia web in qualsiasi browser.
- Pannello di controllo mobile per i dispositivi Android/iOS.
- Possibilità di realizzare criteri di sicurezza individuali per una concreta azienda o per singoli gruppi di dipendenti.
- Possibilità di assegnare amministratori separati a diversi gruppi, il che permette di utilizzare il Pannello di controllo sia in aziende con gli elevati requisiti di sicurezza, che in imprese multisede.
- Possibilità di impostare criteri di sicurezza per qualsiasi tipo di utente, inclusi utenti mobili, e per ogni postazione – anche per una che al momento non è online, il che consente di fornire una protezione sempre attuale in qualsiasi momento.
- Le impostazioni sono protette dalle modifiche da parte dell'utente.
- Possibilità di bloccare l'accesso ai supporti rimovibili, alle risorse della rete locale e di Internet, il che protegge da azioni accidentali o intenzionali degli utenti.
- Possibilità di proteggere le reti che non hanno connessione a Internet.
- Gli agent possono essere installati sulle postazioni in un modo conveniente per l'amministratore – tramite Active Directory, script di avvio, strumenti di installazione remota.

- L'installazione è possibile anche quando un nodo della rete è chiuso e non è accessibile attraverso l'interfaccia web di amministrazione del Pannello di controllo.
- Possibilità di utilizzare la maggior parte dei database esistenti.
- Come database esterni, si possono utilizzare Oracle, PostgreSQL, Microsoft SQL Server, qualsiasi DBMS con supporto di SQL-92 tramite ODBC.
- Possibilità di scrivere propri gestori eventi, il che dà l'accesso diretto alle interfacce interne del Pannello di Controllo.
- Apertura — tramite questa suite l'amministratore di sistema può installare e sincronizzare prodotti aggiuntivi di terze parti, il che anche riduce i costi di costruzione dei sistemi di sicurezza informatica.
- Il sistema di controllo dello stato di protezione è chiaro, la ricerca delle postazioni nella rete è molto efficiente e comoda.
- La possibilità di selezionare una lista dei componenti del prodotto da aggiornare e quella di controllare il passaggio alle nuove versioni permettono agli amministratori di installare solo gli aggiornamenti necessari e provati nelle loro reti.

Link utili

Descrizione:
http://products.drweb.com/enterprise_security_suite/control_center

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

Licenze di Dr.Web Desktop Security Suite

Tipi di licenze

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

I prodotti Dr.Web Desktop Security Suite si possono acquistare separatamente o come una parte del gruppo Dr.Web Enterprise Security Suite. Nel secondo caso si acquistano anche le licenze del Pannello di Controllo di Dr.Web Enterprise Security Suite (tranne gli scanner a linea di comando) e del Crittografo (solo per Dr.Web per Windows).

Varianti di licenze

	Windows 10/8/8.1/7/Vista SP2/XP SP2+ (a 32 bit). Windows 10/8/8.1/7/Vista SP2 (a 64 bit).		Windows 10/8/8.1/7/Vista SP2/XP SP2+ (a 32 bit). Windows 10/8/8.1/7/Vista SP2 (a 64 bit).	Linux	macOS	MS DOS, OS/2
Licenza di base	Protezione integrata	Antivirus	KATANA	Antivirus		
Elementi protettivi della licenza di base	■ Antivirus ■ Antispyware ■ Antirootkit ■ Antispam ■ Antivirus web ■ Controllo d'ufficio ■ Firewall	■ Antivirus ■ Antis-pyware ■ Antirootkit ■ Firewall	■ Un antivirus non basato su firme ■ Dr.Web Cloud ■ Pannello di controllo	■ Antivirus ■ Antispyware	■ Antivirus ■ Antis-pyware ■ Antirootkit	■ Antivirus ■ Antis-pyware ■ Antirootkit
Elementi complementari						
Pannello di controllo	+	+	+*	+	+	–

* Dr.Web KATANA BE.

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

Sistemi operativi supportati

Dr.Web per Windows	Dr.Web per Linux	Dr.Web per macOS	Dr.Web scanner a linea di comando
Antivirus, Protezione integrata: Windows 10/8/8.1/7/Vista SP2/XP SP2+ (a 32 bit). Windows 10/8/8.1/7/Vista SP2 (a 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)	macOS 10.7 e superiore	Windows, MS DOS, OS/2
KATANA: Windows 10/8/8.1/7/Vista SP2/XP SP2+ (a 32 bit). Windows 10/8/8.1/7/Vista SP2 (a 64 bit).			

Dr.Web per Windows

Protezione di workstation, client di terminal server, client di virtual server, client di sistemi incorporati

Vantaggi

- **Disponibilità dei certificati d'approvazione**
  Dr.Web per Windows possiede i certificati d'approvazione rilasciati dal Servizio Federale di Sicurezza e dal Servizio Federale di Controllo Tecnico e di Esportazione della Russia. Questo significa che il programma può essere utilizzato negli enti che richiedono un livello elevato di sicurezza informatica. Dr.Web per Windows è completamente conforme alle prescrizioni della legge sulla protezione di dati personali concernenti prodotti antivirus. Esso può essere usato nelle reti che richiedono il massimo grado di protezione.
- **Licenze flessibili**
  Dr.Web per Windows ha licenze estremamente flessibili con molteplici varianti. Il cliente può acquistare solo i componenti di protezione che gli servono senza dover pagare moduli o intere soluzioni che resteranno inutilizzate.
- **Gestione centralizzata**
  Per proteggere le workstation in modalità centralizzata serve una licenza del Pannello di Controllo di Dr.Web Enterprise Security Suite. Il Pannello di Controllo funziona con la stessa affidabilità nelle reti di qualsiasi dimensione e complessità - sia nelle reti semplici che consistono di pochi computer, sia nelle intranet distribuite che contano migliaia di unità.
- **Protezione completa dalle minacce esistenti**
  Dr.Web per Windows offre una protezione sicura contro la maggior parte delle minacce esistenti. La qualità insuperata di cura e l'alto livello di auto-difesa non lasciano nessuna chance ai virus e altri malware di penetrare nella rete protetta. La presenza di un firewall incorporato e della funzione Office Control (nella licenza "Protezione integrata") non solo impedisce ai virus di infiltrarsi attraverso vulnerabilità di sistemi operativi e programmi, ma consente di controllare in modo affidabile l'operatività delle applicazioni installate.
- **Incremento di produttività del lavoro**
  L'introduzione del software Dr.Web per Windows produce subito un effetto positivo. La riduzione del flusso di spam (nel caso della licenza "protezione integrata") consente ai dipendenti di lavorare con maggiore efficienza (i messaggi importanti non andranno persi tra i messaggi indesiderati). Diventerà impossibile l'infezione della rete e non si dovrà interrompere il lavoro.
- **Mantiene la credibilità dell'azienda**
  Dr.Web per Windows non lascia che i malintenzionati trasformino la rete locale in una fonte di virus e spam.

Funzioni chiave

- Una soluzione complessa per la protezione dei PC Windows.
- Protezione in modalità online.
- Possibilità di installazione e di funzionamento su un computer già infettato, e straordinaria resistenza ai virus.
- Rilevamento efficace di ogni tipo di minaccia e pulizia del sistema.
- Alta velocità di scansione grazie all'utilizzo delle possibilità dei sistemi multiprocessore.
- Protegge dai programmi malevoli nuovi che non possono essere rilevati tramite i tradizionali metodi di analisi basata sulle firme antivirali e di analisi euristica.
- Protezione dei dati contro la corruzione da parte di un trojan-encoder.
- Analisi integrata delle minacce compresse.
- Scansione completa degli archivi di qualsiasi livello di nidificazione.
- Il migliore rilevamento e neutralizzazione dei virus compositi.
- Filtraggio dello spam e dei tutti i tipi di messaggi indesiderati senza la necessità di istruire l'antispam.
- Scansione completa «al volo» di qualsiasi traffico dati su tutte le porte.
- Navigazione sul web sicura con 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 del traffico dati in messaggi istantanei.
- Protezione efficace dei minori contro i contenuti indesiderati.
- Possibilità di impedire l'utilizzo non autorizzato dei dispositivi rimovibili e del computer.
- Servizio basato su cloud Dr.Web Cloud — controllo di URL sui server Doctor Web.
- Protegge il computer dall'accesso non autorizzato dall'esterno, previene la fuga delle informazioni importanti, impedisce le connessioni non attendibili a livello di pacchetti e di applicazioni.
- Possibilità di gestire Dr.Web installato sugli altri computer in una rete locale senza dover installare il Pannello di controllo Dr.Web.

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).

Link utili

Description : http://products.drweb.com/win/workstations

Dr.Web Antivirus per macOS

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

Vantaggi

- Protezione sicura contro tutti i programmi malevoli.
- Alta velocità di scansione antivirus grazie alla tecnologia di scansione asincrona
- Un utile Pannello di controllo che viene concesso in licenza gratis
- Facile integrazione con il sistema di protezione antivirus centralizzata dell'azienda
- Il carico minimo sul sistema protetto e il basso consumo di banda durante l'aggiornamento rende quasi impercettibile il funzionamento di Dr.Web per macOS
- Un'interfaccia di gestione intuitiva e chiara

Possibilità

- Gestione centralizzata delle impostazioni di tutti i componenti.
- Controllo continuo di tutti gli oggetti a rischio di infezione — dispositivi rimovibili, formati di email, cartelle e file, inclusi quelli in packer e in archivi compressi.
- Protezione contro le minacce sconosciute tramite la ricerca non basata sulle firme antivirali Origins Tracing™ e l'analisi euristica intellettuale Dr.Web.
- Rilevamento e rimozione dei programmi malevoli nascosti sotto packer sconosciuti tramite la tecnologia FLY-CODE™.
- Neutralizzazione dei virus, dei trojan e degli altri generi di oggetti malevoli.
- Ampi database per il rilevamento dei programmi spyware, riskware, adware, hacktool e joke.
- È molto resistente ai tentativi dei programmi malevoli di ostacolare o di fermare il funzionamento del file monitor SpIDer Guard®.
- È possibile proteggere da password le impostazioni di SpIDer Guard dalle modifiche non autorizzate.
- Scansione antivirus avviata manualmente, automaticamente o secondo un calendario.
- Scelta del tipo di scansione: rapida, completa e personalizzata.
- Agli oggetti infetti, sospetti o altri vengono applicate le azioni, inclusa la cura, lo spostamento in quarantena e l'eliminazione, anche quando la prima azione selezionata risulta impossibile.
- L'utente può escludere dalla scansione determinati percorsi e file.
- Novità della versione 10! Scansione completa del traffico dati HTTP e controllo dell'accesso a risorse Internet.
- Isolamento in quarantena dei file infetti con la possibilità di impostare il tempo di conservazione degli oggetti e la dimensione massima della quarantena.
- Cura, ripristino o eliminazione degli oggetti spostati in quarantena.
- Vengono registrati l'ora di un evento, l'oggetto scansionato e il tipo di azione applicata.
- Scaricamento degli aggiornamenti in automatico (secondo un calendario) oppure on demand.
- Avvisi automatici (anche tramite segnali sonori) su eventi di virus.
- Registrazione di un dettagliato log di funzionamento. I moduli dell'antivirus sono disponibili come le utility a riga di comando con la possibilità di incorporarle in Apple Scripts in

Requisiti di sistema

- macOS 10.7 o superiore (a 32 e a 64 bit).
- Processore Intel.
- Memoria operativa — a seconda dei requisiti del SO
- Accesso a Internet per registrare il prodotto e ricevere
- gli aggiornamenti.

Link utili

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

Dr.Web Antivirus per Linux

Protezione indispensabile contro i virus

Vantaggi

- Centro di controllo funzionale.
- Possibilità del controllo "al volo".
- Le impostazioni di controllo possono essere personalizzate
- dall'utente.
- Quarantena gestibile.
- Aggiornamenti automatici.
- Interfaccia moderna.
- Scansione completa del traffico dati HTTP e controllo dell'accesso a risorse Internet.
- Protezione dalle minacce per SO Windows eseguite sotto SO Linux.

Possibilità

- Gestione centralizzata delle impostazioni di tutti i componenti.
- Controllo continuo di tutti gli oggetti a rischio di infezione – dispositivi rimovibili, formati di email, cartelle e file, inclusi quelli in packer e in archivi compressi.
- Protezione contro le minacce sconosciute tramite la ricerca non basata sulle firme antivirali Origins Tracing™ e l'analisi euristica intellettuale Dr.Web.
- Rilevamento e rimozione dei programmi malevoli nascosti sotto packer sconosciuti tramite la tecnologia FLY-CODE™.
- Neutralizzazione dei virus, dei trojan e degli altri generi di oggetti malevoli.
- Ampi database per il rilevamento dei programmi spyware, riskware, adware, hacktool e joke.
- L'architettura della soluzione è stata sviluppata appositamente per ridurre il carico sulla CPU e il consumo della memoria.
- **Novità!** Possibilità di installazione, configurazione e funzionamento dell'antivirus senza utilizzo di interfaccia grafica.
- È molto resistente ai tentativi dei programmi malevoli di ostacolare o di fermare il funzionamento di SpIDer Guard.
- **Novità!** Scansione multi-thread che consente di accelerare il funzionamento del programma su processori multi-core.
- Possibilità di scegliere il tipo di scansione antivirus: rapida, completa o personalizzata – può essere avviata manualmente, automaticamente o secondo un calendario.
- **Novità!** Controlla processi in esecuzione per neutralizzare le minacce attive, incluse le minacce per SO Windows avviate tramite Wine.
- Agli oggetti infetti, sospetti o altri vengono applicate le azioni, inclusa la cura, lo spostamento in quarantena e l'eliminazione, anche quando la prima azione selezionata risulta impossibile.
- L'utente può escludere dalla scansione determinati percorsi e file.
- **Novità!** Scansione completa del traffico dati HTTP e controllo dell'accesso a risorse Internet
- Isolamento in quarantena dei file infetti con la possibilità di impostare il tempo di conservazione degli oggetti e la dimensione massima della quarantena.
- Cura, ripristino o eliminazione degli oggetti spostati in quarantena.
- Vengono registrati l'ora di un evento, l'oggetto scansionato e il tipo di azione applicata.
- Scaricamento degli aggiornamenti in automatico (secondo un calendario) oppure on demand.
- **Novità!** Le modifiche delle impostazioni dell'antivirus e della chiave di licenza vengono accettate «al volo».
- Avvisi automatici (anche tramite segnali sonori) su eventi di virus.
- I moduli dell'antivirus sono disponibili come le utility a riga di comando e possono essere utilizzati dall'utente.
- **Inoltre:**
  È possibile utilizzare l'antivirus negli enti che richiedono l'elevato livello della sicurezza.

Requisiti di sistema

- Plateforme : support complet du système de commandes du processeur x86 en modes 32- et 64- bits.
- Espace libre sur le disque dur : au moins 90 Mo.
- Système d'exploitation: fichiers d'installation GNU/Linux avec la version du noyau 2.6.x.
- Accès à Internet : pour enregistrement et la réception des mises à jour.

Link utili

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

Dr.Web Scanner a linea di comando

Protezione antivirus automatizzabile, destinata agli utenti con maggiore esperienza

Gli scanner Dr.Web a linea di comando senza interfaccia grafica usano il database di virus comune e il modulo di ricerca Dr.Web e sono progettati per i sistemi operativi MS DOS, OS/2 e Windows. Per gestire questo tipo di protezione antivirus è necessaria un'adeguata conoscenza della linea di comando.

Vantaggi

- Requisiti di sistema minimi – gli scanner a linea di comando funzionano bene persino in sistemi incorporati e sono in grado di proteggere efficacemente computer di piccola potenza di precedenti generazioni.
- Controllo conveniente – l'amministratore può scegliere la scansione "manuale" oppure quella secondo il calendario.
- Ripulisce 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 numerose capacità 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 un CD o una chiavetta USB).

Link utili

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

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 macOS Server
- Dr.Web per Novell NetWare server
- Dr.Web per Unix (Samba) server

	Dr.Web per Windows server	Dr.Web per Novell Net-Ware server	Dr.Web per Unix server	Dr.Web per macOS Server
Licenza di base	Antivirus			
Elementi complementari				
Pannello di controllo	+	+	+	+

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

Sistemi operativi supportati

Dr.Web per Server Windows	Dr.Web per Server Novell NetWare	Dr.Web per macOS Server	Dr.Web per Server UNIX
Microsoft Windows Server 2000* / 2003 (x32 e x64*) / 2008 / 2012 (x64)	Novell NetWare versione 3.12-6.5 con le addizioni installate Minimum patch list	macOS Server 10.7 e superiori	Distribuzione con il nucleo Linux versioni 2.6.x (sistemi a 32 e a 64 bit)

Dr.Web per Windows Server

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

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 su server aventi pressoché qualsiasi 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 possono scegliere gli oggetti da controllare, le azioni da eseguire in caso di individuazione di virus o file sospetti.
- Il programma è facile da installare e da gestire.
- Garantisce la massima protezione subito dopo l'installazione (con le impostazioni predefinite).
- Trasparenza – genera i file di rapporti dettagliati con i dati richiesti dall'amministratore.

Funzioni principali

- Un consumo premuroso delle risorse del sistema che tiene conto delle capacità hardware.
- Dr.Web Cloud – una reazione istantanea alle attuali minacce.*
- Un sistema della scansione silenziosa e della neutralizzazione di minacce attive.*
- Protezione preventiva – consente di proteggersi dalle minacce ancora sconosciute, vietando le modifiche degli oggetti critici di Windows e controllando azioni insicure.*
- Scansione fatta "al volo" – direttamente quando i file vengono aperti o memorizzati sul server dalle postazioni.
- Protezione del funzionamento del nucleo di sistema e dei propri moduli contro i guasti e i programmi malevoli.
- Ripristina automaticamente i suoi componenti dal repository locale.
- Scansione multi-thread.
- Avviso istantaneo dell'amministratore, di altri utenti e gruppi circa incidenti di virus – via email o via un messaggio inviato al numero telefonico.
- I file infetti vengono isolati in quarantena.
- Pulisce, recupera e/o elimina i file messi in quarantena.
- I database dei virus si aggiornano automaticamente.

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

* Disponibile per i sistemi operativi Windows Server 2008 e superiori.

** Supportati solo per la versione 7.0.

Dr.Web per Novell NetWare Server

La protezione antivirus dei depositi di file

Vantaggi

- Un'ampia gamma di versioni di Novell NetWare supportate – dalla 4.11 alla 6.5.
- Supporta lo spazio dei nomi NetWare.
- Scansione di vasti flussi di dati ad alta velocità con il carico minimo sul sistema operativo.
- Facile da installare.
- Ha una struttura di 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.

Funzioni 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.

Requisiti di sistema

- Novell Netware dalla versione 4.11 alla versione 6.5.

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 di impostazioni flessibile e orientata sui client nella quale si possono scegliere gli oggetti da controllare, le azioni da eseguire in caso si trovino 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.

Funzioni principali

- Verifica i volumi di server secondo il calendario prestabilito oppure su richiesta dell'amministratore.
- Migliorato! Scansione fatta "al volo" – direttamente quando i file sono memorizzati oppure aperti sul server dalle workstation.
- Controllo multi-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, ricupera e/o elimina i file messi in quarantena.
- Mantiene il registro delle attività antivirus.
- I database dei virus si aggiornano automaticamente.

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).

Requisiti di sistema

- Samba 3.0. e superiore.

Link utili

Descrizione: http://products.drweb.com/fileserver/UNIX

Dr.Web per macOS Server

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

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.

Funzioni principali

- Verifica gli oggetti in 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 modifica non autorizzata.
- Applicazione delle azioni per gli oggetti infetti, potenzialmente sospetti e di altro tipo, inclusi la pulitura, lo spostamento in quarantena e l'eliminazione, anche se l'azione prescelta si sia verificata impossibile da eseguire.
- 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 di oggetti in quarantena e la dimensione massima della quarantena.
- Pulisce, recupera oppure elimina gli oggetti spostati in quarantena.
- Mantiene rapporti dettagliati sulle operazioni eseguite.
- I moduli sono accessibili sotto forma di utilità a linea di comando e possono essere incorporati nei sistemi di servizio Apple Scripts.

Requisiti di sistema

- macOS Server 10.7 e superiore.
- Processore Intel.
- Memoria operativa — a seconda dei requisiti del SO
- Accesso a Internet per registrare il prodotto e ricevere gli aggiornamenti.

Link utili

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

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)

Licenze di Dr.Web Mail Security Suite

Tipi di licenze

- Licenza secondo il numero degli utenti protetti (illimitato).
- Licenza per server – scansione illimitata del traffico e-mail sul server fino ad un massimo di 3000 utenti.

I prodotti Dr.Web per la protezione della posta elettronica si possono acquistare separatamente o come una parte del pacchetto Dr. Web Enterprise Suite. Nel secondo 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	Antivirus	Antivirus	Antivirus
Elementi complementari				
Antispam	+*	+	+	–
SMTP proxy	+	+	+	+
Pannello di controllo	+	+	+	+

* Non supportato per MS Exchange 2013.

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

Sistemi operativi supportati

Prodotto Dr.Web	Windows	Linux	macOS	FreeBSD	Solaris
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 (versioni a 32 e 64 bit)	Red Hat Enterprise Linux (RHEL) versioni 4 e 5, Novell SuSE Linux Enterprise Server (SLES) 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	macOS 10.7 e superiori		

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))

Vantaggi

- Possibilità di configurare il software in un modo flessibile secondo le esigenze degli utenti.
- Non richiede un altro livello di qualifica dell'amministratore.
- Alta velocità di risposta.
- Addizionali vantaggi dell'antispam Dr.Web.
- Protezione delle informazioni confidenziali.
- Comoda amministrazione.
- Carattere aperto.
- Possibilità di connettere un numero illimitato di plugin.

Funzioni principali

- Filtraggio dei messaggi email alla ricerca di virus e di spam.
- Scompone i messaggi email e ne analizza tutte le parti.
- Elaborazione corretta della maggioranza dei tipi di 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.
- **Dr.Web per Unix mail server.** La possibilità di archiviare tutti i messaggi e-mail consente di usare questo prodotto come parte dei sistemi informatici degli istituti di credito.
- **Possibilità di configurare il programma con flessibilità 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 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 può dimenticare".
- **Alta velocità di risposta**
  La tecnologia di controllo multi-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 a 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 danneggiare le aziende inserendo con 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 aggiornamenti voluminosi.

Protezione delle informazioni riservate

Il prodotto permette di recuperare i messaggi che gli utenti hanno rimosso inavvertitamente 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 con 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.

Funzioni chiave

- Protezione contro gli attacchi di spammer grazie alla possibilità di limitare i parametri di una sessione SMTP.
- Protezione dallo spam mascherato grazie alla funzione del controllo dell'autenticità di un indirizzo IP.
- Protezione contro gli attacchi di hacker – una protezione efficace sia dagli attacchi passivi (del genere PLAIN, LOGIN ecc.) che dagli attacchi attivi senza utilizzo di dizionario.
- Protezione contro le trappole di spam.
- Protezione contro i messaggi formati incorrettamente.
- Risparmio del traffico Internet perché è possibile limitare la dimensione di allegati.
- Limitazione dei server Open Relays.

SO supportati

- Distribuzioni Linux con la versione del nucleo 2.4.x e superiori.
- FreeBSD versioni 6.x e superiori per le piattaforme Intel x86 e amd64.
- Solaris versione 10 per le piattaforme Intel x86 e amd64.

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

- 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 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 il dispositivo del raggruppamento che rende possibile impostare diversi parametri per vari gruppi d'impiegati e pertanto aiuta a mettere in funzione 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 multi-thread.
- Tecnologie uniche del rilevamento dei programmi di compressione e degli oggetti maligni sconosciuti (anche nuovissimi).
- l'applicazione si avvia automaticamente con l'avvio del sistema operativo.
- Comoda ricezione degli aggiornamenti tramite lo schedulatore Windows.

Funzioni principali

- Verifica "al volo" i messaggi email, compresi i file allegati, alla ricerca di virus e spam.
- Monitoraggio antivirus dei messaggi trovati nelle caselle 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 nella 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

Nel caso si usi 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 (versioni Standard, Enterprise oppure Datacenter) con SP1 installato e superiore.

Nel caso si usi 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.ru/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 standalone, ma anche sui server partitions e sui cluster Lotus Domino. Le copie dell'antivirus che si trovano su differenti partizioni agiscono nella memoria del computer in modo autonomo usando i database e i file eseguibili comuni. In questo caso serve una sola copia di licenza, 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 sistema 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 una 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.

Funzioni principali

- Verifica e filtra "al volo" o su 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.
- Controlla oggetti a richiesta grazie alla funzione manuale che consente di avviare e terminare l'esecuzione di task 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 da danneggiamenti.
- 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.

Version 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

Description : 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 e-mail server Kerio, il che è stato comprovato dai test 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 e-mail server Kerio, il che è molto importante nel caso delle forniture per gli enti pubblici.
- Impegna un tempo minimo per consegnare i messaggi e ha un grado di sicurezza elevato grazie alla tecnologia del controllo multi-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.
- È 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.

Funzioni 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 macOS

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

Link utili

Description : 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
- Dr.Web per Microsoft ISA Server

Licenze di Dr.Web Gateway Security Suite

Tipi di licenze

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

I prodotti Dr.Web per la protezione dei gateway si possono acquistare separatamente o come parte del gruppo Dr.Web Enterprise Security Suite. Nel secondo 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	Dr.Web per Microsoft ISA Server e Fore-front TMG
Licenza di base	Antivirus	Antivirus	Antivirus	Antivirus	Antivirus
Elementi complementari					
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.

Sistemi operativi supportati

Prodotto Dr.Web	Windows	Linux	FreeBSD	Solaris
		per la piattaforma Intel x86		
Dr.Web per Unix Internet Gateway		con la versione del nucleo 2.4.x e superiori	versione 6.x e superiore	versione 10
Dr.Web per Kerio Internet Gateway	2000/ XP/2003/2008/7			
Dr.Web per Microsoft ISA Server e Forefront TMG	**Per Microsoft ISA** Server: Microsoft® Windows Server® 2003 x86 Service Pack 1 (SP1); Microsoft® Windows Server® 2003 R2 x86 **Per Microsoft Forefront** TMG: Microsoft® Windows Server® 2008 SP2 Microsoft® Windows			
Dr.Web per MIMEsweeper	2000 Server SP4 e superiori / Server 2003 e superiori			
Dr.Web per Qbik WinGate	Vista/Server 2008/ Server 2003/XP/2000 (a 32 e 64 bit)			

Dr.Web per Unix Internet Gateway

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

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.
- Alta scalabilità.
- Capacità di elaborare in tempo reale enormi flussi d'informazioni.
- 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.

Funzioni 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.

Sistemi operativi supportati

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

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

- Squid di almeno 3.0.
- 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. Si 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 multi-thread.

Funzioni 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 di malware).
- Registra errori ed eventi nel giornale di eventi (Event Log) e nel giornale in formato testuale.
- Spedisce le notifiche su vari eventi agli utenti prescelti.
- I database virus sono aggiornati in modo automatico.

Requisiti di sistema

Version per Windows

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

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

- Almeno 290 MB di spazio su disco rigido
- Sistema operativo Kerio Control VMware Virtual Appliance o Kerio Control Software Appliance
- Firewall:
  Kerio Control 8.x o 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 filtraggio dei contenuti ClearSwift MIMEsweeper

Vantaggi

- **Semplice da installare e configurare**

  I mezzi di configurazione incorporati in Dr.Web per MIMEsweeper – che sono procedure guidate di scenari – permettono di creare in 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 di 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 disinfetta 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.

Funzioni principali

- Verifica i messaggi postali e i loro allegati, anche gli archivi, prima della loro elaborazione da parte del servermail.
- 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

- Almeno 35 Mb di spazio libero sul disco.
- Sistema operativo Windows 2000 SP4 e superore 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

Vantaggi

- Solo Dr.Web per Qbik WinGate possiede 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 dal formato sconosciuto distingue il prodotto Dr.Web dai suoi concorrenti.

Funzioni 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.
- Conserva un giornale di eventi.
- Ha un proprio pannello di controllo e un gestore della quarantena.
- Aggiornamenti automatici dei database dei virus.

Link utili

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

Dr.Web per Microsoft ISA Server e Forefront TMG

Controllo antivirus e antispam del traffico trasmesso con Microsoft ISA Server e Forefront TMG

Vantaggi

- Controlla qualsiasi oggetto entro un tempo minimo perché utilizza tecnologie di analisi dinamica per valutare le esigenze di risorse che hanno gli altri servizi del server ed è in grado di passare istantaneamente da un compito a un altro in modo automatico.
- Usa le capacità modernissime delle piattaforme per accelerare la velocità del controllo.
- È in grado di funzionare su server di qualsiasi configurazione – anche con una piccola quantità di memoria operativa.
- Protezione di server sia reali, sia virtuali.
- Il componente antispam incorporato che non richiede training (agisce subito dal momento d'installazione) comporta la diminuzione del carico imposto al server e la crescita del rendimento dei dipendenti dell'azienda.
- Blocca l'accesso a diverse risorse di Internet e consentedi filtrare i dati secondo i tipi di file, perciò l'azienda può evitare l'infiltrazione di virus da siti noti come fonti di malware e ridurre il volume di traffico.
- Tecnologie uniche di rilevamento di packer e di oggetti malevoli sconosciuti (nuovissimi).
- Ampie possibilità d'installazione e di messa a punto del software a seconda delle esigenze dell'azienda.
- Documentazione esauriente.

Funzioni principali

- Controllo antivirus e antispam di tutto il traffico trasferito, compresi i file allegati.
- Possibilità di controllare "al volo" i file in transizione con la possibilità di rilevare oggetti malevoli nei file che sono stati compressi più volte.
- Cura i file infetti.
- Applica diverse azioni a seconda del tipo di spam.
- Inserisce un testo di spiegazione nei messaggi di posta che contenevano minacce alla sicurezza informatica.
- Blocca l'accesso ai dati infetti per tutti gli utenti di reti locali.
- Limita l'accesso degli utenti a risorse di Internet tramite il componente Office Control .
- Mette in quarantena i file infetti e sospetti.
- Informa l'amministratore sugli incidenti di virus.
- Registra le informazioni statistiche sul funzionamento del software.
- Aggiornamenti automatici.

Funzioni principali

Per utilizzare Microsoft ISA Server:

- Processore Pentium III 733 MHz e superiore.
- RAM: 1 Gb o maggiore.
- Spazio disponibile sul disco rigido: 300 Mb per l'installazione. È necessario uno spazio disco aggiuntivo per memorizzare temporaneamente i dati nel corso della scansione antivirale.
- S.O.: Microsoft® Windows Server® 2003 x86 con Service Pack 1 (SP1), Microsoft® Windows Server® 2003 R2 x86.
- Server proxy: Microsoft® ISA Server 2004, Microsoft® ISA Server 2006.

Per utilizzare Microsoft Forefront TMG:

- Processore Pentium III 1.86 MHz o superiore.
- RAM: 2 Gb o maggiore.
- Lo spazio disponibile sul disco rigido: 300 Mb per l'installazione. È necessario uno spazio disco aggiuntivo per memorizzare temporaneamente i dati nel corso della scansione antivirale.
- S.O.: Microsoft® Windows Server® 2008 SP2, Microsoft® Windows Server® 2008 R2.
- Server proxy: Microsoft® Forefront® TMG 2010.

Link utili

Descrizione:
http://www.drweb.com/products/gateway/isa

Dr.Web Mobile Security Suite

La protezione dei dispositivi mobili

- Dr.Web per Android
- Dr.Web per BlackBerry

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 Android	Dr.Web per BlackBerry
■ Protezione completa + Pannello di controllo	■ Protezione completa

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

	Dr.Web per Android	Dr.Web per BlackBerry
Componenti di protezione*	Antivirus Antispam** Antifurto** Filtro URL Firewall Auditor della sicurezza	Antivirus Auditor della sicurezza
Protezione centralizzata come parte di Dr.Web Enterprise Security Suite	+	+
Sistemi operativi supportati	Android OS 4.0–7.1 Firewall funziona su Android 4.0 e superiori Android TV 5.0+	BlackBerry 10.3.2+
Funzionalità principali		
Una scansione a più flussi con la distribuzione dei task tra i nuclei del processore	+	
Scansione dei file in arrivo attraverso le connessioni GPRS/Infrared/Bluetooth/Wi-Fi/USB o la sincronizzazione con il PC	+	+
Due tipi di scansione: completa e personalizzata	+	+
Possibilità di attivare/disattivare la scansione continua della scheda di memoria Ripristino dell'operatività in automatico	+	
Scansione on demand di tutto il file system o di singoli file e cartelle	+	
Verifica dei file in archivi APK, ZIP, SIS, CAB, RAR, JAR	+	+
Divieto dell'esecuzione sul dispositivo mobile delle applicazioni non incluse nella lista di quelle consentite dall'amministratore	+	+
Configurazione delle regole di funzionamento per ciascun'applicazione	+	
Controllo immediato del traffico in entrata e uscita per ciascun'applicazione	+	
Possibilità di limitare il traffico per l'uso di Internet mobile	+	
Possibilità di impostare limitazioni a specifiche applicazioni nel roaming Prevenzione dell'accesso a risorse Internet sconsigliate	+	
Protezione da accessi non autorizzati a connessione a reti wireless Sblocco dai trojan-ransomware	+	
Scanner delle vulnerabilità	+	
White e black list di chiamate ed SMS in arrivo	+	
Supporto di più SIM attendibili	+	
Eliminazione dei file infetti	+	+
Spostamento dei file sospetti in quarantena	+	+
Ripristino dei file da quarantena	+	+
Aggiornamento via Internet: ■ attraverso il protocollo HTTP con l'utilizzo del modulo GPRS incorporato; ■ attraverso le connessioni Infrared/Bluetooth/Wi-Fi/USB; ■ sincronizzando con un PC connesso a Internet attraverso la connessione ActiveSync	+	+
Report dettagliati sulla scansione del sistema	+	+
Le informazioni circa le minacce trovate vengono collocate sul pannello di blocco da cui è possibile pas- sare alla lista delle minacce	+	
Avviso sul rilevamento di azioni proprie dei programmi malevoli	+	
Gestione remota del dispositivo mobile in caso di smarrimento o furto – tramite Antifurto	+	
Ottenimento via SMS delle coordinate GPS del dispositivo mobile	+	

Link utili

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

* Per i dispositivi Android TV sono disponibili soltanto Antivirus, Firewall e Auditor della sicurezza.

** Non è possibile utilizzare questo componente sui dispositivi senza slot per schede SIM.

Pacchetti Dr.Web

I pacchetti Dr.Web comprendono prodotti specifici per la protezione di tutti gli oggetti informatici.

Important! 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 a prezzo intero. Lo sconto sul rinnovo viene concesso solo se l'utente passa da un pacchetto a 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 agevoli, 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

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	■ Disinfettare in modo centralizzato e remoto le workstation e i server Windows. ■ Valutare la qualità della protezione antivirale fornita da un altro produttore.
Caratteristiche dell'utilità	■ Non è necessario rimuovere l'antivirus dell'altro produttore prima di controllare e disinfettare il computer. ■ Non c'è bisogno di avere un server o installare ancora altro software. ■ L'utilità si può usare nelle reti che sono completamente isolate da Internet. ■ Il wizard Dr.Web CureNet! può essere avviato da qualsiasi supporto removibile, tra cui anche chiave USB.
Descrizione del prodotto	http://curenet.drweb.com/
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), iPhone 4, iPod touch 4 iOS 7.0+.
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.
Requisiti di sistema	**Wizard** ■ 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) ■ RAM libera: almeno 360 MB ■ Spazio libero su disco rigido: almeno 200 MB ■ Connessione con tutte le postazioni da scansionare attraverso il protocollo TCP/IP ■ Accesso ad Internet: per l'aggiornamento dei database dei virus e dei componenti di Dr.Web CureNet! **Scanner** ■ 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 ■ RAM libera: almeno 360 MB ■ Spazio libero su disco rigido: almeno 200 MB

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.

Utenti potenziali	Piccole e medie imprese, su cui computer e server è già stato installato l'antivirus di un altro produttore.
Obiettivi raggiungibili	■ Disinfettare immediatamente le workstation e i server Windows. ■ Valutare la qualità della protezione antivirale fornita da un altro produttore.
Caratteristiche dell'utilità	■ 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. ■ Autodifesa incrementata e regime potenziato per reagire efficacemente ai Trojan.Winlock. ■ Aggiornamenti una o più volte l'ora. ■ L'utilità può essere avviata da qualsiasi supporto remov bile, tra cui anche chiave USB.
Descrizione del prodotto	http://free.drweb.com/cureit
Sistemi operativi supportati	MS Windows 10/8/7/Vista/2012/2008 (sistemi a 32 e 64 bit), XP/2003 (sistemi a 32 bit).
Licenze	L'utility viene concessa in licenza per 12, 24 e 36 mesi.
Particolarità di licenze	L'utilità è gratuita per curare il proprio PC di casa.
Versione demo	Non è disponibile.

Russia

Dr.Web S.r.l.

Russia, 125040, Mosca, via 3 Yamskogo Polya, tenuta 2, edificio 12A

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

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

www.drweb.ru | curenet.drweb.ru | www.av-desk.com | free.drweb.ru

China

Doctor Web Software Company (Tianjin), Ltd.

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

天津市经济技术开发区第四大街80号软件大厦北楼112

Telefono / fax: +86-022-59823480

www.drweb.cn

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

Kazakistan

TOO "Doctor Web – Tsentralnaya Asia"

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

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

www.drweb.kz

Ucraina

Centro del supporto tecnico "Doctor Web"

Ucraina, 01601, Kiev, via Pushkinskaya, 27, ufficio 6

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

www.drweb.ua

Francia

Doctor Web France

333 b Avenue de Colmar, 67100 Strasbourg, France

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

www.drweb.fr

Japan

Doctor Web Pacific, Inc.

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

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

www.drweb.co.jp