Dr.WEB

Server Security Suite (macOS)

Manuale dell'utente

© Doctor Web, 2025. Tutti i diritti riservati

Il presente documento ha carattere puramente informativo e indicativo nei confronti del software della famiglia Dr.Web in esso specificato. Il presente documento non costituisce una base per conclusioni esaustive sulla presenza o assenza di qualsiasi parametro funzionale e/o tecnico nel software della famiglia Dr.Web e non può essere utilizzato per determinare la conformità del software della famiglia Dr.Web a qualsiasi requisito, specifica tecnica e/o parametro, nonché ad altri documenti di terze parti.

I materiali riportati in questo documento sono di proprietà Doctor Web e possono essere utilizzati esclusivamente per uso personale dell'acquirente del prodotto. Nessuna parte di questo documento può essere copiata, pubblicata su una risorsa di rete o trasmessa attraverso canali di comunicazione o nei mass media o utilizzata in altro modo tranne che per uso personale, se non facendo riferimento alla fonte.

Marchi

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA e il logotipo Dr.WEB sono marchi commerciali registrati di Doctor Web in Russia e/o in altri paesi. Altri marchi commerciali registrati, logotipi e denominazioni delle società, citati in questo documento, sono di proprietà dei loro titolari.

Disclaimer

In nessun caso Doctor Web e i suoi fornitori sono responsabili di errori e/o omissioni nel documento e di danni (diretti o indiretti, inclusa perdita di profitti) subiti dall'acquirente del prodotto in connessione con gli stessi.

Dr.Web Server Security Suite (macOS)
Versione 12.6
Manuale dell'utente
1/31/2025

Doctor Web, Sede centrale in Russia

Indirizzo: 125124, Russia, Mosca, 3a via Yamskogo polya, 2, 12A

Sito web: https://www.drweb.com/

Telefono +7 (495) 789-45-87

Le informazioni sulle rappresentanze regionali e sedi sono ritrovabili sul sito ufficiale della società.

Doctor Web

Doctor Web — uno sviluppatore russo di strumenti di sicurezza delle informazioni.

Doctor Web offre efficaci soluzioni antivirus e antispam sia ad enti statali e grandi aziende che ad utenti privati.

Le soluzioni antivirus Dr.Web esistono a partire dal 1992 e dimostrano immancabilmente eccellenza nel rilevamento di programmi malevoli, soddisfano gli standard di sicurezza internazionali.

I certificati e premi, nonché la vasta geografia degli utenti testimoniano la fiducia eccezionale nei prodotti dell'azienda.

Siamo grati a tutti i nostri clienti per il loro sostegno delle soluzioni Dr.Web!

Sommario

1. Dr.Web Server Security Suite (macOS)

1.1. Segni convenzionali e abbreviazioni

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
Rete antivirus	Un nuovo termine o un termine accentato nelle descrizioni.
<indirizzo_IP>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
`/Volumes/Macintosh HD/`	Nomi di file e directory, frammenti di codice.
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

1.2. Sull'applicazione

Dr.Web protegge il Mac in modo affidabile da qualsiasi tipo di minaccia: virus, rootkit, trojan, spyware, adware, hacktool e vari oggetti malevoli utilizzando le più moderne tecnologie di rilevamento e neutralizzazione dei virus.

I componenti Dr.Web vengono costantemente aggiornati, i database dei virus e i database delle categorie di risorse web vengono regolarmente integrati con nuove firme delle minacce. Gli aggiornamenti mantengono aggiornata la protezione del dispositivo. Per la neutralizzazione delle minacce sconosciute, vengono utilizzati i metodi di analisi euristica.

Funzioni principali

- scansione continua di tutti i file sul Mac;
- scansione del sistema su richiesta dell'utente;
- scansione dei dati trasmessi attraverso il protocollo HTTP non sicuro;
- controllo delle connessioni delle applicazioni alla rete e blocco delle connessioni sospette;
- protezione della fotocamera e del microfono da accessi non autorizzati (solo sui dispositivi con macOS 10.13 e versioni precedenti).

Informazioni sull'applicazione

Per aprire la finestra con le informazioni sull'applicazione, nell'angolo superiore sinistro della finestra principale dell'applicazione fare clic sull'icona .

Le informazioni sull'applicazione sono raggruppate in cinque schede:

- **Informazioni su Dr.Web** — versione dell'applicazione, versione del motore antivirus, data dell'ultimo aggiornamento, identificatore del dispositivo, opzione di generazione del report per il supporto tecnico, se tale parametro è attivato nella sezione Impostazioni generali.
- **Aiuto** — guida all'utilizzo di Dr.Web.
- **Notizie** — ultime notizie che vengono pubblicate sul sito dell'azienda Doctor Web.
- **Promozioni** — promozioni effettuate dall'azienda Doctor Web.
- **Sui virus** — notizie sui virus rilevati dagli analisti Doctor Web.

1.3. Requisiti di sistema

Parametro	Requisiti
Dispositivo	Mac con sistema operativo macOS
Spazio su disco rigido	2 GB
Sistema operativo	• OS X 10.11 El Capitan; • macOS 10.12 Sierra; • macOS 10.13 High Sierra; • macOS 10.14 Mojave; • macOS 10.15 Catalina; • macOS 11 Big Sur; • macOS 12 Monterey; • macOS 13 Ventura; • macOS 14 Sonoma; • macOS 15 Sequoia.

Per il corretto funzionamento di Dr.Web devono essere aperte le seguenti porte:

Scopo	Direzione	Numeri di porte
Per l'attivazione e il rinnovo della licenza	in uscita	443
Per l'aggiornamento	in uscita	80
Per la connessione al servizio cloud Dr.Web Cloud	in uscita	UDP: • 2075

Scopo	Direzione	Numeri di porte
		TCP: • 3010, • 3020, • 3030, • 3040

Come scoprire la versione del sistema operativo del Mac

1. Andare al menu Apple .
2. Premere **Informazioni su questo Mac**.
3. (Solo per i dispositivi con macOS 12 e versioni precedenti) Selezionare la scheda **Panoramica**.

Come scoprire quanto spazio libero c'è sul Mac

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Informazioni su questo Mac**.
3. Premere **Archiviazione**. Si vedrà la quantità di spazio libero sul Mac.

Se si vogliono visualizzare raccomandazioni per l'ottimizzazione dello spazio di archiviazione, premere **Gestisci**.

Per macOS 13.0 e versioni successive

1. Selezionare il menu Apple > **Impostazioni di sistema**.
2. Sulla barra laterale a sinistra premere **<%GENERAL_MAC%>**.
3. A destra selezionare **Archiviazione**. Si vedrà la quantità di spazio libero sul Mac.

Inoltre, nella sezione **<%RECOMMENDATIONS_MAC%>** si troveranno consigli sull'ottimizzazione dello spazio di archiviazione.

2. Installazione e rimozione

Installazione di Dr.Web

Per installare Dr.Web

1. Scaricare il file di installazione dal sito https://download.drweb.com/mac/.
2. Avviare il file.
3. Premere **Installa Dr.Web**.
4. Premere **Avanti**. Inizierà il processo di installazione dell'applicazione.
5. Inserire la password dell'account e premere **Installa programma ausiliario**.
6. Alla comparsa dell'avviso **Estensione di sistema bloccata** consentire il caricamento delle estensioni di sistema.
7. Dr.Web verrà copiato nella cartella **Applicazioni** e verrà avviato.
8. Concedere a Dr.Web i permessi per l'accesso completo al disco.

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web Ltd.

Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione**

prima di poter essere utilizzati e premere **Dettagli** sotto.

5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa fare clic sull'icona ⓘ.
7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

Per concedere i permessi per l'accesso completo al disco

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Passare alla sezione **Sicurezza e privacy**.
5. Passare alla sezione **Privacy**.
6. Premere **Accesso al disco**.
7. Aggiungere i moduli Dr.Web alla lista di quelli consentiti.
8. Premere **Riavvia**.

Per macOS 13.0 e versioni successive

1. Nella finestra principale Dr.Web fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Premere **Consenti**.
4. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
5. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando

non verrà visualizzata l'icona Dr.Web.

6. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
7. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
8. Premere **Riavvia** per salvare le modifiche.

> Se il pulsante **Consenti** è inattivo, l'accesso al disco è già consentito.

Al termine dell'installazione sul pannello superiore macOS comparirà l'icona . Apre la finestra principale Dr.Web.

Durante il primo avvio, Dr.Web aggiornerà i database dei virus allo stato attuale. Successivamente Dr.Web aggiorna i database dei virus ogni 30 minuti. È possibile modificare la frequenza di aggiornamento.

Errori durante l'installazione

Sistema operativo non supportato

Dr.Web può essere installato solo su un Mac con una versione supportata del sistema operativo macOS. Aggiornare il sistema operativo.

Come scoprire la versione del sistema operativo del Mac

1. Andare al menu Apple .
2. Premere **Informazioni su questo Mac**.
3. (Solo per i dispositivi con macOS 12 e versioni precedenti) Selezionare la scheda **Panoramica**.

Memoria insufficiente su disco

Per installare Dr.Web, sono richiesti circa 2 GB di spazio libero su disco.

Come scoprire quanto spazio libero c'è sul Mac

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Informazioni su questo Mac**.
3. Premere **Archiviazione**. Si vedrà la quantità di spazio libero sul Mac.

Se si vogliono visualizzare raccomandazioni per l'ottimizzazione dello spazio di archiviazione, premere **Gestisci**.

Per macOS 13.0 e versioni successive

1. Selezionare il menu Apple > **Impostazioni di sistema**.
2. Sulla barra laterale a sinistra premere **<%GENERAL_MAC%>**.
3. A destra selezionare **Archiviazione**. Si vedrà la quantità di spazio libero sul Mac.

Inoltre, nella sezione **<%RECOMMENDATIONS_MAC%>** si troveranno consigli sull'ottimizzazione dello spazio di archiviazione.

È installato un altro antivirus

Dr.Web non è compatibile con altre applicazioni antivirus. Inoltre, non è possibile installare due versioni di Dr.Web su un solo Mac.

L'installazione di due antivirus su un solo computer può portare a errori di sistema e perdite di dati importanti. Pertanto, prima di installare Dr.Web, è necessario rimuovere la sua versione precedente o altri antivirus installati.

Informazioni su come rimuovere un antivirus di terze parti possono essere trovate nei materiali di consultazione o sul sito ufficiale dell'applicazione installata.

Errore n.

Contattare il supporto tecnico dell'azienda Doctor Web. Allegare alla richiesta il log di installazione che si trova nella cartella `\Library\DrWeb`.

Lista degli errori

Rimozione di Dr.Web

1. In **Finder** trovare l'applicazione **Disinstalla Dr.Web** e avviarla.
2. Inserire il nome e la password dell'utente.
3. Dr.Web verrà rimosso dalla cartella **Applicazioni**.

Dopo la rimozione di Dr.Web sul Mac rimangono i file della chiave e di configurazione e il file con le impostazioni dell'applicazione.

Non utilizzare applicazioni di terze parti per la rimozione di Dr.Web. Ciò può portare alla rimozione incompleta dell'applicazione.

Se l'applicazione non è stata rimossa per intero, è possibile rimuoverla manualmente.

Per rimuovere Dr.Web manualmente

Inserire uno dopo l'altro i seguenti comandi in **Terminale**:

```
sudo /usr/bin/killall 'Dr.Web for macOS'

sudo /bin/launchctl remove com.drweb.pro.configd

sudo /bin/launchctl remove com.drweb.LoginLauncher

sudo rm -f /Library/PrivilegedHelperTools/com.drweb.agent

sudo rm -f /Library/LaunchDaemons/com.drweb.agent.plist

sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove '/Library/Application Support/DrWeb/bin/drweb-gated'

sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove '/Library/Application Support/DrWeb/bin/drweb-firewall'

sudo /sbin/kextunload -m com.drweb.kext.DrWebNetMonitor

sudo /sbin/kextunload -m com.drweb.kext.DrWebMonitor

sudo /bin/launchctl remove com.drweb.agent

sudo "/Applications/Dr.Web/Dr.Web for macOS.app/Contents/Resources/Extensions/Dr.Web Firewall.app/Contents/MacOS/Dr.Web Firewall" --deactivate

sudo "/Applications/Dr.Web/Dr.Web for macOS.app/Contents/Resources/Extensions/Dr.Web Spider.app/Contents/MacOS/Dr.Web Spider" --deactivate

sudo rm -Rf /usr/local/bin/drweb-ctl
```

```
sudo rm -Rf "/Library/LaunchDaemons/com.drweb.pro.configd.plist"

sudo rm -Rf "/Library/LaunchAgents/com.drweb.LoginLauncher.plist"

sudo rm -Rf "/Library/Application Support/DrWeb/mail"

sudo rm -Rf "/Library/Application Support/DrWeb/html"

sudo rm -Rf "/Library/Application Support/DrWeb/dws"

sudo rm -Rf "/Library/Application Support/DrWeb/var/drl"

sudo rm -Rf "/Library/Application Support/DrWeb/bases"

sudo rm -Rf "/Library/Application Support/DrWeb/lib"

sudo rm -Rf "/Library/Application Support/DrWeb/bin"

sudo rm -Rf "/Library/Application Support/DrWeb/version"

sudo rm -Rf "/Library/Application Support/DrWeb/var"

sudo rm -Rf "/Library/Application Support/DrWeb/www"

sudo rm -Rf "/Library/Application Support/DrWeb/update/Library/Application
Support/DrWeb/cache/esagent"

sudo rm -Rf "/Library/Application Support/DrWeb/cache/cloud"

sudo rm -Rf "/Library/Application Support/DrWeb/cache"

sudo rm -Rf "/Library/Application Support/DrWeb/install.plist"

sudo rm -Rf "/Applications/Dr.Web/Dr.Web for macOS.app"

sudo rm -Rf "/Applications/Dr.Web/Uninstall Dr.Web.app"

sudo rm -Rf /Applications/Dr.Web
```

3. Accesso completo al disco

Affinché i componenti Dr.Web possano svolgere le proprie funzioni e proteggere il Mac, è necessario consentire all'applicazione *l'accesso completo al disco*.

Questo può essere fatto

- passando dagli avvisi sulla necessità di consentire l'accesso,
- nelle impostazioni Dr.Web, sezione **Generali**.

> All'aggiornamento del sistema operativo a macOS 13 Ventura, sarà necessario consentire nuovamente l'accesso al disco.

Se l'accesso al disco non verrà consentito, il Mac dopo ogni riavvio visualizzerà una finestra a comparsa con un avviso su quello che l'applicazione richiede l'accesso.

Configurazione dell'accesso completo al disco

Dalle impostazioni

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Premere **Consenti**.
4. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
5. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando non verrà visualizzata l'icona Dr.Web.
6. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
7. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
8. Premere **Riavvia** per salvare le modifiche.

> Se il pulsante **Consenti** è inattivo, l'accesso al disco è già consentito.

Passando da un avviso

1. Premere **Consenti**.

2. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
3. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando non verrà visualizzata l'icona Dr.Web.
4. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
5. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
6. Premere **Riavvia** per salvare le modifiche.

Per concedere l'accesso completo al disco attraverso le preferenze di sistema del Mac senza usare la Procedura guidata di concessione dell'accesso al disco, sarà necessario trascinare manualmente nella finestra delle preferenze tutti i componenti di Dr.Web. Per evitare errori, consigliamo di usare la Procedura guidata.

4. Gestione delle licenze

Per il funzionamento di Dr.Web è necessaria una licenza che può essere acquistata sul sito dell'azienda Doctor Web o dai partner. La licenza consente di utilizzare tutte le funzionalità dell'applicazione durante l'intero periodo di validità. La licenza regola i diritti dell'utente in conformità al Contratto di licenza le condizioni di cui l'utente accetta durante l'installazione dell'applicazione.

A ciascuna licenza è assegnato un numero di serie univoco, e sul computer è archiviato un file speciale con i parametri della licenza. Questo file è chiamato file della chiave di licenza.

Se prima di acquistare una licenza si vuole conoscere le funzionalità di Dr.Web, è possibile attivare una versione di prova. Nella versione di prova sono disponibili tutte le funzioni e i componenti di protezione.

4.1. Versione di prova

Se prima di acquistare una licenza si vuole conoscere le funzionalità di Dr.Web, è possibile attivare una versione di prova. Fornisce le piene funzionalità dei componenti principali, ma il suo periodo di validità è limitato.

> Una versione di prova può essere attivata sullo stesso computer solo una volta all'anno.

È possibile attivare una versione di prova:

- Di 1 mese. La registrazione e il numero di serie non sono richiesti. La licenza verrà attivata automaticamente.

Per attivare la versione di prova

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Nella sezione **Attivazione della licenza** andare al link **Ottieni versione di prova per 30 giorni**.

4.2. Acquisto della licenza

Se non si dispone di una licenza valida Dr.Web, è possibile acquistare una nuova licenza sulla pagina del negozio online Doctor Web.

Per acquistare una nuova licenza

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Acquista**. Si aprirà una pagina del sito dell'azienda Doctor Web su cui è possibile procedere con l'acquisto.

Dopo il completamento dell'acquisto all'indirizzo che è stato indicato per la registrazione arriverà un'email con il numero di serie e il file della chiave (in allegato).

4.3. Attivazione della licenza

Per utilizzare tutte le funzioni e i componenti dell'applicazione, attivare la licenza. Si consiglia di attivare la licenza immediatamente dopo l'installazione dell'applicazione. Ciò è necessario per l'aggiornamento dei database dei virus e il funzionamento dei componenti dell'applicazione, per esempio, la protezione continua del file system, la protezione dalle minacce di rete e la scansione del traffico web.

La finestra di attivazione compare automaticamente quando si avvia Dr.Web per la prima volta. È possibile avviare l'attivazione in un secondo momento nella sezione **Licenza** della finestra principale dell'applicazione. L'attivazione delle licenze è possibile tramite il file della chiave, il numero di serie o il file di configurazione (.cfg).

Come attivare la licenza tramite il numero di serie

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Attiva**.
3. Nella finestra **Attivazione della licenza** inserire il numero di serie.
4. Premere il pulsante **Attiva**.
5. Nel modulo di registrazione inserire il proprio nome, la regione e l'indirizzo email. Queste informazioni saranno richieste per il ripristino della licenza, se sarà necessario. Premere il pulsante **Registrati**.

Come attivare la licenza tramite il file della chiave

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Attiva**.
3. Nella finestra **Attivazione della licenza** aprire la scheda **File di attivazione**.
4. Trascinare il file della chiave di formato `.key` nell'area tratteggiata o fare clic per selezionare il file sul Mac.
5. Nel modulo di registrazione inserire il proprio nome, la regione e l'indirizzo email. Queste informazioni saranno richieste per il ripristino della licenza, se sarà necessario. Premere il pulsante **Registrati**.

Domande ricorrenti

Come posso trasferire la licenza su un altro computer?

È possibile trasferire la licenza su un altro computer tramite il file della chiave o il numero di serie.

Per trasferire la licenza su un altro computer

- tramite il numero di serie:
  1. Rimuovere Dr.Web dal computer da cui si vuole trasferire la licenza, o attivare un'altra licenza su questo computer.
  2. Attivare la licenza corrente sul computer su cui si vuole trasferire la licenza tramite il numero di serie. È possibile attivare la licenza durante l'installazione o durante il funzionamento dell'applicazione.
- tramite il file della chiave:
  1. Copiare il file della chiave dal computer da cui si vuole trasferire la licenza. Di default il file della chiave è archiviato nella cartella di installazione Dr.Web e ha l'estensione `.key`.
  2. Rimuovere Dr.Web dal computer da cui si vuole trasferire la licenza, o attivare un'altra licenza su questo computer.
  3. Attivare la licenza corrente sul computer su cui si vuole trasferire la licenza tramite il file della chiave. È possibile attivare la licenza durante l'installazione o durante il funzionamento dell'applicazione.

Non può essere trasferita su un altro computer la licenza ricevuta per l'attivazione della versione di prova dell'applicazione.

Ho dimenticato l'indirizzo email di registrazione. Come posso ripristinarlo?

Se si è dimenticato l'indirizzo email fornito per la registrazione, contattare il supporto tecnico dell'azienda Doctor Web.

Se si fa una richiesta da un indirizzo diverso da quello a cui è registrata la licenza, l'addetto al supporto tecnico può chiedere di fornire: una copia fotografica o scannerizzata del certificato di licenza, lo scontrino di pagamento della licenza, l'email del negozio online e altri documenti di conferma.

Come posso modificare l'indirizzo email di registrazione?

Se si vuole modificare l'indirizzo email fornito per la registrazione, utilizzare un servizio speciale sul sito dell'azienda Doctor Web.

4.4. Rinnovo della licenza

È possibile rinnovare la licenza corrente nella sezione **Attivazione della licenza**.

Come rinnovare la licenza se non è ancora scaduta

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Acquista**. Si aprirà una pagina del sito dell'azienda Doctor Web su cui è possibile procedere con l'acquisto.

Come rinnovare la licenza se è scaduta

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Acquista**. Si aprirà una pagina del sito dell'azienda Doctor Web su cui è possibile procedere con l'acquisto.

Dr.Web supporta l'aggiornamento al volo che non richiede la reinstallazione dell'applicazione o l'interruzione del suo funzionamento. Per aggiornare la licenza Dr.Web, attivare la nuova licenza.

Per attivare la licenza

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Attiva**.
3. Nella finestra **Attivazione della licenza**:
   - Inserire il numero di serie e premere il pulsante **Attiva**.
   - Se si ha un file della chiave, aprire la scheda **File di attivazione**. Trascinare il file nell'area tratteggiata o fare clic per selezionare il file sul Mac.

Le istruzioni dettagliate su come attivare la licenza sono disponibili nella sezione Attivazione della licenza.

Se la licenza che si vuole rinnovare è scaduta, Dr.Web inizierà a utilizzare la nuova licenza.

Se la licenza che si vuole rinnovare non è ancora scaduta, il numero di giorni rimanenti verrà automaticamente aggiunto alla nuova licenza. Allo stesso tempo, la licenza precedente verrà bloccata. Sull'indirizzo email che è stato indicato per la registrazione arriverà un avviso corrispondente.

4.5. Ripristino della licenza

Se il file della chiave è stato perso o danneggiato, il funzionamento di tutti i componenti Dr.Web viene bloccato, e la sicurezza del Mac può essere a rischio. Per la riattivazione della licenza, ripristinare il file della chiave utilizzando il numero di serie.

Come ripristinare il file della chiave

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere il pulsante **Attiva**.
3. Nella finestra **Attivazione della licenza** inserire il numero di serie e premere il pulsante **Attiva**.

Alla riattivazione viene rilasciato lo stesso file della chiave che si è ricevuto in precedenza.

Come ripristinare il numero di serie

Se non si è riusciti a trovare il numero di serie, è possibile ripristinarlo nei seguenti modi:

- Contattare il venditore della licenza (se è stata acquistata una versione diversa dalla versione in scatola).
- Utilizzare il modulo di ripristino sul sito dell'azienda Doctor Web.
- Contattare il supporto tecnico dell'azienda Doctor Web. Allegare alla richiesta una conferma della titolarità della licenza secondo queste regole.

È possibile attivare nuovamente la licenza a condizione che non sia scaduta.

Il file della chiave di licenza può essere ottenuto tramite l'applicazione un numero di volte limitato. Se questo numero è superato, si può ottenere il file della chiave confermando la registrazione del numero di serie sul sito https://products.drweb.com/register/. Il file della chiave verrà inviato all'indirizzo email che è stato indicato durante la prima registrazione.

4.6. Numero di serie

A ciascuna licenza corrisponde un *numero di serie* univoco. Per il suo tramite la licenza Dr.Web può essere attivata.

Come scoprire il numero di serie

Se il numero di serie non è registrato

- Se la licenza è stata acquistata in un negozio online, il numero di serie può essere trovato nell'email del negozio online sull'acquisto della licenza.
  - Se la licenza è stata acquistata nel negozio online dell'azienda Doctor Web, il numero di serie può essere trovato nella Sezione personale sul sito Allsoft.ru nei dati sull'ordine.
  - Se la licenza è stata acquistata nel negozio online dell'azienda Doctor Web attraverso l'account sul sito ed è stata dichiarata nel programma fedeltà, il numero di serie può essere trovato nel servizio I miei acquisti.
- Se è stata acquistata la versione in scatola, il numero di serie può essere trovato nel Certificato di licenza incluso nella scatola.
- Se la licenza è stata acquistata in una catena di vendita al dettaglio, il numero di serie può essere trovato sullo scontrino.

Se il numero di serie è registrato

- Se Dr.Web è installato sul Mac, scaricare questo file e aprirlo. Fare doppio clic sul file `YSN.cmd`. Verrà creato un file di testo `YourSerialNumber.txt` che si aprirà automaticamente nell'editor di testo. Tutti i numeri di serie sono elencati dopo il prefisso "SN=".
- Se Dr.Web non è installato, ripristinare il numero di serie tramite un modulo sul sito dell'azienda Doctor Web.

Se Dr.Web viene utilizzato in abbonamento

In questo caso non è richiesto il numero di serie o il file della chiave.

- Se l'abbonamento è stato acquistato sul sito dell'azienda Doctor Web, l'identificatore (ID) dell'abbonamento può essere trovato nella sezione I miei abbonamenti.
- Se l'abbonamento è stato acquistato da un altro fornitore, l'ID dell'abbonamento può essere trovato nell'area personale sul sito del fornitore di servizi informatici.

Come ripristinare il numero di serie

Se non si è riusciti a trovare il numero di serie, è possibile ripristinarlo nei seguenti modi:

- Contattare il venditore della licenza (se è stata acquistata una versione diversa dalla versione in scatola).
- Utilizzare il modulo di ripristino sul sito dell'azienda Doctor Web.
- Contattare il supporto tecnico dell'azienda Doctor Web. Allegare alla richiesta una conferma della titolarità della licenza secondo queste regole.

4.7. File della chiave

Il file della chiave definisce il tipo di licenza e i diritti dell'utente all'uso di Dr.Web.

Il file della chiave di licenza ha l'estensione `.key`. Può essere ottenuto nel corso dell'attivazione della licenza.

Il file della chiave contiene informazioni:

- sulla lista dei componenti che l'utente può utilizzare;
- sul periodo durante cui Dr.Web può essere utilizzato;
- sulla presenza o l'assenza del supporto tecnico;
- su altre limitazioni (in particolare, il numero di computer su cui può essere utilizzato Dr.Web).

Il file della chiave deve essere nella cartella di installazione Dr.Web. L'applicazione controlla regolarmente la presenza e la correttezza del file della chiave. Per non violare l'integrità del file della chiave, non aprirlo negli editor di testo e non modificarlo.

In assenza di un file della chiave valido, l'attività di tutti i componenti Dr.Web viene bloccata.

Il file della chiave Dr.Web è *valido* se sono contemporaneamente soddisfatte le seguenti condizioni:

- la licenza non è scaduta,
- l'integrità della chiave non è violata.

Se è violata qualsiasi delle condizioni, il file della chiave diventa *non valido*, in tale caso, Dr.Web interrompe la neutralizzazione dei programmi malevoli.

Conservare il file della chiave fino alla scadenza della licenza o della versione di prova. Se Dr.Web viene installato su più computer o viene reinstallato, può essere utilizzato il file della chiave di licenza ottenuto alla prima attivazione.

Il file della chiave ottenuto per l'attivazione della versione di prova può essere utilizzato solo sul computer su cui è stata effettuata la registrazione.

5. Pannello di controllo

Sulla scheda **Pannello di controllo** della finestra principale dell'applicazione è possibile:

- configurare il funzionamento dei componenti di protezione,
- avviare la scansione antivirus del Mac,
- impostare i parametri di accesso alla fotocamera e al microfono (solo sui dispositivi con macOS 10.13 e versioni precedenti),
- aggiornare manualmente i database dei virus,
- scoprire informazioni sulla licenza attuale,
- visualizzare informazioni sulle minacce rilevate.

Componenti di protezione

- SpIDer Guard — monitor del file system. Verifica in tempo reale tutti i file a cui accedono gli utenti e controlla le applicazioni e i processi in esecuzione sul Mac.
- SpIDer Gate — monitor di internet. Verifica il traffico HTTP e controlla l'accesso a risorse internet.
- Firewall — firewall. Protegge il Mac da accessi non autorizzati dall'esterno e fughe di dati importanti attraverso la rete.

Controlla Mac

Scanner — il componente principale per il rilevamento dei virus che può eseguire:

- la scansione del sistema su richiesta dell'utente: rapida, completa o personalizzata;
- la neutralizzazione delle minacce rilevate (cura, rimozione, spostamento in quarantena). È possibile selezionare manualmente l'azione richiesta o impostare l'applicazione automatica dell'azione specificata nelle impostazioni per questo tipo di minaccia.

Protezione della privacy

- **Fotocamera** — controllo dell'accesso delle applicazioni alla fotocamera.
- **Microfono** — controllo dell'accesso delle applicazioni al microfono.

> Le impostazioni di controllo dell'accesso alla fotocamera e al microfono sono assenti su macOS 10.14 e versioni successive.

Aggiornamento

Selezionare la voce **Nessun aggiornamento richiesto**/**Aggiornamento richiesto** per aggiornare manualmente i database dei virus. Nei database dei virus sono contenute informazioni su tutti i programmi malevoli conosciuti.

Licenza

Nella sezione **Licenza** sono raccolte informazioni sulla licenza attuale:

- stato della licenza,
- numero,
- nome del titolare,
- data di attivazione,
- data di scadenza,
- numero di giorni rimanenti.

È possibile attivare una licenza se si ha già un numero di serie, un file della chiave o di configurazione, o acquistare una nuova licenza.

Minacce

- Minacce — lista generale delle minacce rilevate. È possibile rimuovere, spostare in quarantena o ignorare queste minacce.
- Quarantena — una cartella speciale che si usa per isolare i file infetti e altre minacce affinché non possano causare danno al sistema.

6. Avvisi

Sulla scheda **Avvisi** della finestra principale dell'applicazione vengono visualizzate le seguenti informazioni su Dr.Web e sul suo funzionamento:

- stato della licenza;
- informazioni sul rilevamento delle minacce e sulla loro neutralizzazione;
- stato dei database dei virus;
- informazioni sugli errori nel funzionamento dei componenti di protezione;
- stato della connessione al server di protezione centralizzata;
- informazioni sui tentativi di connessione al microfono e alla fotocamera;
- messaggi dall'amministratore del server di protezione centralizzata.

> Le informazioni sui tentativi di connessione al microfono o alla fotocamera vengono visualizzate solo sui dispositivi con macOS 10.13 e versioni precedenti.

Dr.Web utilizza gli avvisi di sistema macOS per visualizzare messaggi sul rilevamento delle minacce, la loro neutralizzazione o gli errori nel funzionamento dei componenti. È possibile disattivare o configurare gli avvisi di sistema da Dr.Web.

Per disattivare gli avvisi

1. Andare al menu Apple > **Preferenze di sistema**.
2. Premere **Notifiche e full immersion**.
3. A sinistra nella lista delle applicazioni selezionare Dr.Web per macOS e disattivare gli avvisi utilizzando l'interruttore .

> Su macOS 10.14 e versioni precedenti questo interruttore è assente. Per disattivare gli avvisi, togliere tutti i flag.

Per configurare gli avvisi di sistema

1. Andare al menu Apple > **Preferenze di sistema**.
2. Premere **Notifiche e full immersion**.
3. A sinistra nella lista delle applicazioni selezionare Dr.Web per macOS. Configurare lo stile dei promemoria dell'applicazione e le relative opzioni.

7. Aggiornamento dei database dei virus

Nella sezione **Modulo di aggiornamento** è possibile configurare la frequenza di aggiornamento dei database dei virus. Nei database dei virus sono contenute informazioni su tutti i programmi malevoli conosciuti.

Ogni giorno compaiono nuovi tipi di minacce con funzioni di mascheramento più perfette. L'aggiornamento Dr.Web consente di rilevare i virus precedentemente sconosciuti, bloccarne la propagazione, e in alcuni casi, curare i file infetti precedentemente incurabili. Aggiornare tempestivamente i database dei virus: 24 ore dopo l'ultimo aggiornamento riuscito diventano obsoleti.

Affinché Dr.Web possa aggiornare i database dei virus, è necessaria una connessione internet.

Durante il primo avvio, Dr.Web aggiorna i database dei virus allo stato attuale. Successivamente Dr.Web aggiorna i database dei virus ogni 30 minuti. È possibile modificare la frequenza di aggiornamento.

Per modificare la frequenza di aggiornamento dei database dei virus

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **Modulo di aggiornamento**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  e inserire il nome utente e la password.
4. Nella lista a cascata **Aggiorna i database dei virus** selezionare la frequenza di aggiornamento.

Dr.Web si aggiornerà automaticamente secondo la frequenza di caricamento degli aggiornamenti selezionata.

Inoltre, è possibile avviare manualmente il processo di aggiornamento.

Per aggiornare i database dei virus manualmente

- Nella finestra principale selezionare la voce **Nessun aggiornamento richiesto/Aggiornamento richiesto**.

Dr.Web controllerà e aggiornerà i database dei virus.

Configurazione del server proxy

Se non si vuole che gli aggiornamenti vengano installati sul Mac direttamente, è possibile configurare l'installazione degli aggiornamenti attraverso un server proxy.

Per configurare l'installazione degli aggiornamenti attraverso un server proxy

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Modulo di aggiornamento**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su e inserire il nome utente e la password.
4. Spuntare il flag **Utilizza server proxy**.
5. Premere **Configura proxy**.
6. Indicare l'indirizzo e la porta del server proxy.
7. Se il server proxy richiede una password, spuntare il flag **Proteggi con password il server proxy**.
8. Indicare il nome utente e la password.
9. Premere **Salva**.

8. Protezione del file system continua

Il monitor del file system SpIDer Guard verifica in tempo reale tutti i file a cui accedono gli utenti e controlla le applicazioni e i processi in esecuzione sul Mac.

È possibile escludere singole cartelle e file dalla scansione continua.

SpIDer Guard si avvia automaticamente dopo l'installazione e l'attivazione della licenza Dr.Web. Il monitor funziona continuamente e si avvia all'accensione del Mac.

Al rilevamento delle minacce SpIDer Guard visualizza un messaggio sullo schermo e applica l'azione specificata nelle impostazioni. È possibile modificare le azioni che vengono automaticamente applicate a diversi tipi di minacce o applicare le azioni manualmente.

Attivazione e disattivazione di SpIDer Guard

Il componente SpIDer Guard può essere disattivato solo da utenti con privilegi di amministratore.

Se la protezione antivirus continua è disattivata, evitare di connettersi a internet, nonché aprire file da supporti non controllati da Scanner.

Per sospendere temporaneamente o riprendere la protezione del file system continua

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Componenti di protezione**.
2. Attivare o disattivare il monitor del file system SpIDer Guard utilizzando l'interruttore  .

SpIDer Guard non funziona/Estensione di sistema bloccata

In macOS 10.13 e nelle versioni successive viene bloccato il caricamento delle estensioni di sistema (dei moduli del kernel). In tale caso il componente SpIDer Guard non funziona, e sullo schermo compare un messaggio sul blocco dell'estensione di sistema. Affinché la scansione del file system funzioni correttamente sul Mac, consentire il caricamento del software di sistema Doctor Web Ltd.

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web Ltd.

> Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione prima di poter essere utilizzati** e premere **Dettagli** sotto.
5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa fare clic sull'icona ⓘ.
7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

8.1. Configurazione del monitor di file SpIDer Guard

Nella sezione delle impostazioni **SpIDer Guard** è possibile impostare le azioni che Dr.Web applicherà automaticamente alle minacce in base al loro tipo.

SpIDer Guard cerca di curare i file infetti: oggetti infettati da virus conosciuti e potenzialmente curabili. Gli oggetti sospetti e diversi tipi di programmi malevoli vengono spostati da SpIDer Guard in Quarantena.

È possibile cambiare le azioni che SpIDer Guard applica a ciascun tipo di oggetti malevoli. La scelta delle azioni disponibili dipende dal tipo di minaccia:

Azione	Descrizione
Cura, sposta in quarantena oggetti incurabili	Ripristina lo stato dell'oggetto prima dell'infezione. Se il virus è incurabile o il tentativo di cura non è riuscito, l'oggetto verrà spostato in quarantena. Questa azione è possibile solo per gli oggetti infettati da un virus conosciuto curabile, ad eccezione di trojan e file infetti all'interno di archivi compressi, file di email o container di file.
Cura, rimuovi oggetti incurabili	Ripristina lo stato dell'oggetto prima dell'infezione. Se il virus è incurabile o il tentativo di cura non è riuscito, l'oggetto verrà rimosso. Questa azione è possibile solo per gli oggetti infettati da un virus conosciuto curabile, ad eccezione di trojan e file infetti all'interno di archivi compressi, file di email o container di file.
Rimuovi	Rimuove l'oggetto. Per i settori di avvio non verrà eseguita alcuna azione.
Sposta in quarantena	Isola l'oggetto in una cartella speciale Quarantena. Consente di prevenire perdite accidentali di dati importanti. Per i settori di avvio non verrà eseguita alcuna azione.
Ignora	Salta l'oggetto senza eseguire alcuna azione e visualizzare avvisi. Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.

Le impostazioni predefinite di azioni automatiche non dovrebbero essere modificate senza necessità.

Azioni di SpIDer Guard applicate agli oggetti malevoli rilevati

Tipo di oggetto	Azione				
	Cura, sposta in quarantena oggetti incurabili	Cura, rimuovi oggetti incurabili	Sposta in quarantena	Rimuovi	Ignora
Infetti	+/*	+	+	+	
Sospetti			+/*	+	+
Adware			+/*	+	+
Dialer			+/*	+	+
Joke			+	+	+/*
Riskware			+	+	+/*
Hacktool			+	+	+/*
Archivi infetti	+	+	+	+	+
File di posta infetti	+	+	+	+	+

Segni convenzionali e abbreviazioni

+	azione possibile
+/*	azione impostata di default

Per archivi e file di posta infetti non è possibile impostare un'azione di default, in quanto le azioni vengono applicate ad essi a seconda della minaccia rilevata. Se sono presenti più minacce, l'azione appropriata verrà applicata a quella più significativa.

Per configurare le azioni automatiche

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Guard**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Se necessario, cambiare le azioni automatiche per i tipi di minacce elencati.

Impostazioni aggiuntive

È possibile configurare ulteriormente SpIDer Guard e attivare la scansione degli archivi e dei file di email e impostare il tempo massimo di scansione di un oggetto.

> La modifica di queste impostazioni può portare al rallentamento del Mac e aumentare il tempo di scansione complessivo.

Per attivare la scansione degli archivi e dei file di email

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Guard**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Premere il pulsante **Avanzate**.
5. Attivare le opzioni **Archivi**, **File di email**.
6. Premere **Salva**.

Per impostare il tempo massimo di scansione di un oggetto

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Guard**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Premere il pulsante **Avanzate**.
5. Attivare l'opzione **Tempo massimo di controllo di un oggetto**.
6. Impostare il tempo massimo di scansione di un oggetto in secondi.
7. Premere **Salva**.

8.2. Esclusione di file e cartelle dalla scansione

È possibile escludere singole cartelle e file dalla scansione continua.

Per escludere file e cartelle dalla scansione

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Eccezioni**.

3. Andare alla scheda **File e cartelle**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
5. Premere il pulsante  e indicare la cartella richiesta o un singolo file o trascinarlo nella lista.
6. Premere **Salva**. Ora SpIDer Guard non controllerà questo file.

Se si vuole annullare temporaneamente l'esclusione di un oggetto dalla scansione, ma lasciandolo nella lista, disattivare l'opzione **SpIDer Guard** a destra dell'oggetto.

- Per rimuovere un oggetto dalla lista delle eccezioni, selezionarlo nella lista e fare clic su o trascinarlo fuori dai confini della finestra dell'applicazione.
- Per ripulire la lista delle eccezioni, selezionare tutti gli elementi nella lista (COMANDO-A) e fare clic su  .

Le impostazioni di eccezioni predefinite sono ottimali per la maggior parte degli usi e non dovrebbero essere modificate senza necessità.

Di default tutte le cartelle di quarantena sono aggiunte alla lista delle eccezioni. Queste cartelle sono progettate per isolare oggetti pericolosi perciò l'accesso ad esse è bloccato e non è necessario controllarle.

9. Scansione del traffico web

Ad ogni connessione a internet i browser, gestori di download e altre applicazioni scambiano dati con il server di un determinato sito. I dati in tale caso vengono trasmessi attraverso il protocollo HTTP non sicuro. Il monitor di internet SpIDer Gate esegue la scansione del traffico e blocca la trasmissione di oggetti che possono minacciare la sicurezza del Mac.

SpIDer Gate anche supporta la sciandone dei dati che vengono trasmessi attraverso il protocollo HTTPS sicuro. Per configurare la scansione del traffico cifrato, attivare l'opzione corrispondente nella sezione Rete.

SpIDer Gate si avvia automaticamente dopo l'installazione e l'attivazione della licenza Dr.Web. Il monitor funziona continuamente e si avvia all'accensione del Mac.

SpIDer Gate limita l'accesso ai siti sconsigliati e alle pagine che contengono materiali che violano la legislazione del diritto d'autore. È possibile modificare queste opzioni, e inoltre, definire le impostazioni di accesso a singoli siti e categorie di risorse internet.

È possibile escludere dalla scansione del traffico web singoli siti e le connessioni di rete di applicazioni specifiche.

Attivazione e disattivazione di SpIDer Gate

> Le applicazioni di scansione traffico web e controllo dell'accesso a risorse web di terze parti che sono installate sul Mac potrebbero non funzionare correttamente se è attivato SpIDer Gate.

Per sospendere temporaneamente o riprendere la scansione del traffico web

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Componenti di protezione**.
2. Attivare o disattivare SpIDer Gate utilizzando l'interruttore .

SpIDer Gate non funziona / Estensione di sistema bloccata

In macOS 10.13 e nelle versioni successive viene bloccato il caricamento delle estensioni di sistema (moduli del kernel). In tale caso il componente SpIDer Gate non funziona, e sullo schermo compare un messaggio sul blocco dell'estensione di sistema. Affinché la scansione del traffico web sul Mac funzioni correttamente, consentire il caricamento del software di sistema Doctor Web Ltd.

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web Ltd.

> Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione prima di poter essere utilizzati** e premere **Dettagli** sotto.
5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa fare clic sull'icona ⓘ.
7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

9.1. Configurazione del monitor di internet SpIDer Gate

Nella sezione delle impostazioni **SpIDer Gate** è possibile configurare i parametri di scansione delle minacce di rete e di accesso alle risorse internet.

SpIDer Gate limita l'accesso ai siti sconsigliati e alle pagine che contengono materiali che violano la legislazione del diritto d'autore. Inoltre, SpIDer Gate blocca programmi sospetti, adware e dialer.

È possibile configurare la scansione delle minacce web, creare regole di accesso a singole pagine e selezionare categorie aggiuntive di siti l'accesso a cui sarà limitato.

Le impostazioni predefinite non dovrebbero essere modificate senza necessità.

Scansione delle minacce

Sulla scheda **Controllo delle minacce** è possibile configurare i parametri di scansione delle minacce web, impostare il blocco dei programmi malevoli per tipo e indicare il tempo massimo di scansione di un oggetto.

SpIDer Gate limita l'accesso ai siti sconsigliati e alle URL aggiunte su richiesta dei titolari del diritto. Quali siti sono considerati sconsigliati da Dr.Web?

È possibile togliere le limitazioni sulla visita a questi siti.

Per togliere le limitazioni

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Controllo delle minacce** disattivare le opzioni **Blocca le URL aggiunte su richiesta di titolari del diritto d'autore**, **Blocca siti sconsigliati**, **Blocca oggetti non controllati**.

Di default Dr.Web salta gli oggetti la cui scansione non è riuscita. È possibile attivare il blocco degli oggetti non controllati.

Per attivare il blocco degli oggetti non controllati

1. Nella finestra principale fare clic su  .

2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Controllo delle minacce** attivare l'opzione **Blocca oggetti non controllati**.

Di default SpIDer Gate blocca programmi sospetti, adware e dialer. È possibile configurare il blocco dei tipi di programmi malevoli.

Per configurare il blocco dei programmi malevoli

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Controllo delle minacce** selezionare i tipi di programmi malevoli di cui si vuole bloccare la trasmissione.

È possibile impostare il tempo massimo di scansione di un oggetto.

L'aumento del tempo massimo di scansione di un oggetto può portare al rallentamento del Mac.

Per impostare il tempo massimo di scansione di un oggetto

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Controllo delle minacce** nell'opzione **Tempo massimo di controllo di un oggetto** impostare il tempo massimo di scansione di un oggetto in secondi.

Filtro URL

Sulla scheda **Accesso ai siti** è possibile impostare le regole di accesso a singole pagine e selezionare le categorie di siti l'accesso a cui sarà temporaneamente limitato.

È possibile selezionare le categorie di siti l'accesso a cui sarà temporaneamente limitato indipendentemente dalle altre impostazioni SpIDer Gate.

Per limitare l'accesso alle categorie di siti

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Accesso ai siti** selezionare le categorie di siti l'accesso a cui sarà temporaneamente limitato:

Categoria	Descrizione
Siti per adulti	Siti contenenti materiali pornografici o erotici, siti di incontri, ecc.
Violenza	Siti contenenti esortazioni alla violenza, materiali su vari incidenti con perdita di vite umane ecc.
Armi	Siti dedicati alle armi e agli esplosivi, nonché materiali con la descrizione della loro fabbricazione ecc.
Giochi d'azzardo	Siti che ospitano giochi per soldi online, casinò online, aste, nonché siti di scommesse ecc.
Droga	Siti che propagandano l'uso, la fabbricazione o la distribuzione di sostanze stupefacenti ecc.
Giochi online	Siti che ospitano giochi che utilizzano una connessione internet permanente.
Terrorismo	Siti contenti materiali propagandistici aggressivi, descrizioni di attentati ecc.
Linguaggio volgare	Siti con linguaggio volgare (in titoli di sezioni, articoli ecc.).
Chat	Siti per la messaggistica in tempo reale.
Email	Siti che forniscono la possibilità di registrazione gratuita di una casella email.
Social network	Social network di carattere generale, business, social network aziendali e tematici, nonché siti di incontri tematici.
Anonymizer	Siti che consentono all'utente di nascondere le sue informazioni personali e forniscono accesso a siti bloccati.
<% CRYPTOCURRENCY POOLS%>	Siti che forniscono accesso a servizi che riuniscono utenti con lo scopo di estrazione di criptovalute (mining).
<%JOBS%>	Siti per ricerca lavoro.

È possibile indicare siti l'accesso a cui sarà temporaneamente limitato indipendentemente dalle altre impostazioni SpIDer Gate.

Per limitare l'accesso a un singolo sito

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **SpIDer Gate**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Sulla scheda **Accesso ai siti** fare clic su in fondo alla tabella e inserire l'indirizzo del sito.

9.2. Esclusione di siti dalla scansione

È possibile escludere singoli siti dalla scansione del traffico web. L'accesso a questi siti sarà consentito indipendentemente dalle impostazioni del monitor di internet SpIDer Gate.

Per consentire l'accesso a un determinato sito

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Eccezioni**.
3. Andare alla scheda **Siti**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Fare clic su in fondo alla tabella e inserire l'indirizzo del sito.

- Per rimuovere un oggetto dalla lista delle eccezioni, selezionarlo nella lista e fare clic su o trascinarlo fuori dai confini della finestra dell'applicazione.
- Per ripulire la lista delle eccezioni, selezionare tutti gli elementi nella lista (COMANDO-A) e fare clic su .

9.3. Scansione del traffico cifrato

Ad ogni connessione a internet il Mac scambia dati con il server di un determinato sito. Sempre più servizi web utilizzano le connessioni sicure: lo scambio di informazioni avviene tramite il protocollo HTTPS. La sicurezza in tale caso è fornita dal protocollo crittografico SSL/TLS che supporta la cifratura dati.

Di default Dr.Web non esegue la scansione del traffico cifrato.

Per attivare la scansione del traffico cifrato

1. Nella finestra principale fare clic su .

2. Nella finestra **Preferenze** selezionare la sezione **Rete**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Selezionare **Controlla traffico cifrato**.

Affinché Dr.Web possa controllare il traffico cifrato, il certificato digitale del sito a cui viene stabilita la connessione viene sostituito con il certificato di sicurezza dell'azienda Doctor Web.

Che cos'è un certificato di sicurezza

Certificato di sicurezza — documento elettronico che attesta che il programma è stato testato da una delle autorità di certificazione.

Il certificato di sicurezza garantisce che la comunicazione avvenga in modalità sicura con il controllo dell'autenticità del titolare del certificato.

All'installazione di Dr.Web il certificato di sicurezza dell'azienda Doctor Web viene automaticamente importato nella lista dei certificati di sistema. Tuttavia, alcune applicazioni, per esempio i browser (Opera, Firefox) e i client di posta (Mozilla Thunderbird, The Bat!), non utilizzano l'archivio certificati di sistema.

Per tali applicazioni è possibile esportare manualmente il certificato dell'azienda Doctor Web e quindi installarlo (importarlo) nell'applicazione richiesta.

Per esportare il certificato Doctor Web

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **Rete**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  e inserire il nome utente e la password.
4. Premere il pulsante **Esporta**.
5. Selezionare la cartella in cui si vuole salvare il certificato. Premere **Salva**.
6. Importare il certificato nell'applicazione richiesta. Per maggiori informazioni su come importare un certificato vedere i materiali di consultazione per questa applicazione.

Se dopo aver attivato l'opzione **Controlla traffico cifrato** si riscontrano problemi nel funzionamento dei client di archiviazione cloud (per esempio Google Drive, Dropbox, Yandex.Disk), escludere queste applicazioni dalla scansione.

9.4. Esclusione di applicazioni dalla scansione

È possibile escludere dalla scansione del traffico web le connessioni di rete di determinate applicazioni. Le connessioni per queste applicazioni saranno consentite indipendentemente dalle impostazioni del monitor di internet SpIDer Gate.

Per escludere dalla scansione le connessioni di rete di applicazioni

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Eccezioni**.
3. Andare alla scheda **Applicazioni**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Fare clic su e indicare l'applicazione richiesta o trascinarla nella lista.

- Per rimuovere un oggetto dalla lista delle eccezioni, selezionarlo nella lista e fare clic su o trascinarlo fuori dai confini della finestra dell'applicazione.
- Per ripulire la lista delle eccezioni, selezionare tutti gli elementi nella lista (COMANDO-A) e fare clic su .

10. Protezione dalle minacce di rete

Firewall protegge il Mac da accessi non autorizzati dall'esterno e previene fughe di dati importanti. Consente di controllare le connessioni internet delle applicazioni e il trasferimento dei dati attraverso la rete e blocca le connessioni sospette.

Firewall si avvia automaticamente dopo l'installazione e l'attivazione della licenza Dr.Web. Il componente funziona continuamente e si avvia all'accensione del Mac.

Firewall controlla tutto il traffico in entrata e in uscita e prende decisioni sul blocco o sull'accesso delle applicazioni a risorse di rete secondo la modalità di funzionamento selezionata e le singole regole di filtraggio.

Attivazione e disattivazione di Firewall

Se Firewall è attivato, le applicazioni di scansione del traffico web e controllo dell'accesso a risorse web di terze parti installate sul Mac potrebbero non funzionare correttamente.

Per sospendere temporaneamente o riprendere la protezione dalle minacce di rete

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Componenti di protezione**.
2. Attivare o disattivare Firewall utilizzando l'interruttore .

Firewall non funziona/Estensione di sistema bloccata

Su macOS 10.13 e versioni successive viene bloccato il caricamento delle estensioni di sistema (dei moduli del kernel). In tale caso Firewall non sarà operativo, e sullo schermo comparirà un messaggio sul blocco di un'estensione di sistema. Affinché la protezione dalle minacce di rete funzioni correttamente sul Mac, consentire il caricamento del software di sistema Doctor Web Ltd.

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic

su  in fondo alla finestra e inserire il nome utente e la password.

5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web Ltd.

Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione prima di poter essere utilizzati** e premere **Dettagli** sotto.
5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa fare clic sull'icona ⓘ.
7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

Firewall ha bloccato l'accesso a internet

Se un'applicazione, ad esempio, un browser, non può ottenere l'accesso a internet, creare per essa una regola di permesso nelle impostazioni di Firewall.

10.1. Configurazione di Firewall

Nella sezione delle impostazioni **Firewall** è possibile impostare i parametri di scansione del traffico in arrivo e in uscita e configurare l'accesso delle singole applicazioni alle risorse internet.

Firewall consente l'accesso alle risorse di rete a tutte le applicazioni affidabili. Se un'applicazione non è inclusa nella lista di quelle affidabili, Dr.Web mostra un avviso e chiede quale azione deve essere eseguita.

Quali applicazioni sono considerate affidabili da Dr.Web?

Alle applicazioni affidabili appartengono le applicazioni di sistema macOS, le applicazioni che hanno un certificato di sicurezza o una firma digitale valida. Le regole per tali applicazioni non vengono visualizzate nella lista delle regole di filtraggio.

È possibile modificare la modalità di funzionamento di Firewall e impostare regole di filtraggio per singole applicazioni che non si applicano alla modalità di funzionamento selezionata.

Modalità di funzionamento

Selezionare una delle seguenti modalità di funzionamento:

- **Consenti applicazioni affidabili** — l'accesso alle risorse di rete è consentito a tutte le applicazioni affidabili. Per le altre applicazioni Dr.Web mostra un avviso e chiede quale azione deve essere utilizzata.
- **Consenti tutte le connessioni** — l'accesso alle risorse di rete è consentito a tutte le applicazioni sconosciute. Le connessioni conosciute vengono elaborate da Firewall secondo le regole di filtraggio impostate.
- **Blocca tutte le connessioni** — l'accesso alle risorse di rete è bloccato per tutte le applicazioni sconosciute. Le connessioni conosciute vengono elaborate da Firewall secondo le regole di filtraggio impostate.

Di default sono consentite tutte le connessioni.

Per modificare la modalità di funzionamento di Firewall

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **Firewall**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.

4. Nella parte superiore della finestra nella lista a cascata **Modalità** selezionare la modalità di funzionamento richiesta.

Regole di filtraggio

È possibile creare regole di filtraggio per singole applicazioni. Le regole impostate si applicano indipendentemente dalla modalità di funzionamento di Firewall selezionata.

Una regola di filtraggio è costituita da:

- un file di applicazione di formato `.app`;
- un'azione: consentire o bloccare la connessione;
- un numero di porta su cui viene effettuata la connessione;
- un indirizzo IP, un nome host del sito o server l'accesso a cui verrà controllato da Firewall.

Per creare una nuova regola

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Firewall**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Fare clic su in fondo alla tabella. Si aprirà una finestra per la creazione di una nuova regola.
5. Nel campo **<%ADD APP%>** premere .
6. Selezionare se la regola riguarderà tutte le applicazioni o indicare un'applicazione sul Mac.
7. Seleziona dalla lista a cascata un'azione: **Blocca** o **Consenti**.
8. Indicare il numero di porta su cui viene effettuata la connessione.

   Se il campo **Porta** viene lasciato vuoto, la regola verrà applicata a tutte le porte.

   Eccezione: se si vuole creare una regola che riguarda tutte le applicazioni, l'indicazione del numero di porta è obbligatoria.

9. Nella lista a cascata **Connessione** selezionare:
   - **Qualsiasi server**, se si vuole configurare l'accesso a tutti i server e su tutti gli indirizzi IP.

   Se si vuole creare una regola che riguarda tutte le porte, l'indicazione dell'indirizzo IP o dell'host è obbligatoria.

- **Indirizzo IP**, se si vuole configurare l'accesso a un determinato indirizzo IP. Inserire l'indirizzo in formato IPv4: `192.0.2.235`.
- **Host**, se si vuole configurare l'accesso a un determinato host. Inserire l'host del sito o server in formato `example.com`.

10. Premere il pulsante **Crea**.

Per modificare una regola

1. Nella finestra principale fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **Firewall**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.
4. Nella tabella con le regole di filtraggio fare doppio clic sulla regola richiesta. Si aprirà la finestra di modifica della regola.

    Se per un'applicazione sono create più regole, fare clic su  per espandere la lista.

5. Modificare i parametri di regola necessari.
6. Premere **Salva**.

11. Scansione del Mac su richiesta

Scanner Dr.Web verifica gli oggetti del file system su richiesta dell'utente e rileva le minacce che nascondono la loro presenza nel sistema. Per mantenere il Mac ben protetto, è necessario di tanto in tanto avviare una scansione del sistema tramite Dr.Web.

È possibile escludere singole cartelle e file dalla scansione su richiesta.

> Quando il Mac passa all'alimentazione a batteria, la scansione viene sospesa per rallentare il consumo della carica della batteria. In questo caso Dr.Web chiede all'utente di decidere se continuare o meno la scansione. Al passaggio all'alimentazione da rete elettrica la scansione riprenderà automaticamente.

Per controllare velocemente le parti più vulnerabili del sistema, avviare **Scansione rapida**, mentre per controllare l'intero file system, avviare **Scansione completa**. È inoltre possibile controllare singoli file e cartelle.

Tipi di scansione

Modalità di scansione	Descrizione
Scansione rapida	In questa modalità vengono controllati: • i settori di avvio di tutti i dischi; • la memoria operativa; • la cartella radice del disco di avvio; • la cartella di sistema; • la cartella dell'utente corrente; • i file temporanei; • i punti di ripristino del sistema; • la presenza di rootkit (se il processo di scansione è avviato come amministratore). Gli archivi e i file di email non vengono controllati in questa modalità.
Scansione completa	Scansione completa della memoria operativa e di tutti i dischi rigidi (inclusi i settori di avvio), e inoltre, il controllo della presenza di rootkit.
Scansione personalizzata	Scansione di qualsiasi file e cartella indicata dall'utente.

Per avviare la scansione rapida

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Controlla Mac**.
2. Premere **Scansione rapida**.

Per avviare la scansione completa

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Controlla Mac**.
2. Premere **Scansione completa**.

Per avviare la scansione di singoli file e cartelle

È possibile controllare singoli file e cartelle con qualsiasi dei seguenti metodi.

Attraverso la sezione Controlla Mac

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Controlla Mac**.
2. Trascinare i file e le cartelle che si vogliono controllare nell'area tratteggiata o fare clic in questa area e selezionare gli oggetti da controllare.

Con il trascinamento sull'icona dell'applicazione

1. Trascinare il file o la cartella che si vuole controllare sull'icona Dr.Web nella barra dei menu (situata lungo il margine superiore dello schermo del Mac).

Dal menu contestuale

1. Selezionare il file o la cartella richiesta sul desktop o nel Finder.
2. Richiamare il menu contestuale e premere **Controlla con Dr.Web**.

Risultati della scansione

La finestra con i risultati della scansione diventa disponibile se

- la scansione è stata interrotta (tramite il pulsante **Stop**),
- Dr.Web ha completato la scansione del Mac.

Nella finestra con i risultati della scansione sono indicati:

- il numero di oggetti controllati,
- il numero di oggetti saltati,
- il numero di minacce rilevate,
- il numero di minacce neutralizzate.

Al rilevamento delle minacce Scanner applica le azioni specificate nelle impostazioni. È possibile modificare le azioni che vengono automaticamente applicate a diversi tipi di minacce o applicare le azioni manualmente.

Per visualizzare informazioni dettagliate sulle minacce

- Nella finestra con i risultati della scansione premere il pulsante **Più nel dettaglio**. Si aprirà la scheda **Dettagli di scansione**.

Sulla scheda **Dettagli di scansione** è possibile visualizzare informazioni dettagliate sulle minacce che Dr.Web ha rilevato durante l'ultima scansione.

Perché alcuni oggetti sono stati saltati

Causa	Soluzione
Permessi insufficienti per eseguire l'azione sull'oggetto.	Avviare la scansione con i privilegi di amministratore.
La dimensione del file è troppo grande.	Aumentare il tempo massimo di scansione di un oggetto nelle impostazioni Scanner. Avviare di nuovo la scansione.
Il file è danneggiato o protetto da password.	Se questo è un archivio, decomprimerlo. Avviare di nuovo la scansione.
Nella lista degli oggetti saltati ci sono archivi.	Nelle impostazioni Scanner attivare l'opzione **Archivi** o decomprimere gli archivi. Avviare di nuovo la scansione.
Nella lista degli oggetti saltati ci sono file di email.	Nelle impostazioni Scanner attivare l'opzione **File di email**. Avviare di nuovo la scansione.

Scansione con privilegi di amministratore

Per eseguire le azioni per alcuni oggetti malevoli, l'applicazione Dr.Web può richiedere i privilegi di amministratore.

Per avviare la scansione con i privilegi di amministratore

1. Nella finestra principale fare clic su .

2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.
3. Premere il pulsante **Avanzate**.
4. Selezionare **Avvia scansione come amministratore**.
5. Avviare di nuovo la scansione.

11.1. Configurazione di Scanner

Nella sezione delle impostazioni **Scanner** è possibile impostare le azioni che Dr.Web applicherà alle minacce in base al loro tipo.

Scanner cerca di curare i file infetti: oggetti infettati da virus conosciuti e potenzialmente curabili. Gli oggetti sospetti e i diversi tipi di programmi malevoli vengono spostati da Scanner in Quarantena.

È possibile cambiare le azioni che Scanner applica agli oggetti malevoli. La scelta delle azioni disponibili dipende dal tipo di minaccia:

Azione	Descrizione
Cura, sposta in quarantena oggetti incurabili	Ripristina lo stato dell'oggetto prima dell'infezione. Se il virus è incurabile o il tentativo di cura non è riuscito, l'oggetto verrà spostato in quarantena. Questa azione è possibile solo per gli oggetti infettati da un virus conosciuto curabile, ad eccezione di trojan e file infetti all'interno di archivi compressi, file di email o container di file.
Cura, rimuovi oggetti incurabili	Ripristina lo stato dell'oggetto prima dell'infezione. Se il virus è incurabile o il tentativo di cura non è riuscito, l'oggetto verrà rimosso. Questa azione è possibile solo per gli oggetti infettati da un virus conosciuto curabile, ad eccezione di trojan e file infetti all'interno di archivi compressi, file di email o container di file.
Rimuovi	Rimuove l'oggetto. Per i settori di avvio non verrà eseguita alcuna azione.
Sposta in quarantena	Isola l'oggetto in una cartella speciale Quarantena. Consente di prevenire perdite accidentali di dati importanti. Per i settori di avvio non verrà eseguita alcuna azione.
Ignora	Salta l'oggetto senza eseguire alcuna azione e visualizzare avvisi. Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.

Per modificare le impostazioni di Scanner, non è necessario inserire il nome utente e la password. Le impostazioni cambieranno per tutti gli utenti del Mac automaticamente.

Le impostazioni predefinite di azioni automatiche non dovrebbero essere modificate senza necessità.

Azioni di Scanner applicate agli oggetti malevoli rilevati

Tipo di oggetto	Azione				
	Cura, sposta in quarantena oggetti incurabili	Cura, rimuovi oggetti incurabili	Sposta in quarantena	Rimuovi	Ignora
Infetti	+/*	+	+	+	
Sospetti			+/*	+	+
Adware			+/*	+	+
Dialer			+/*	+	+
Joke			+	+	+/*
Riskware			+	+	+/*
Hacktool			+	+	+/*
Archivi infetti	+	+	+	+	+
File di posta infetti	+	+	+	+	+

Segni convenzionali e abbreviazioni

+	azione possibile
+/*	azione impostata di default

Per archivi e file di posta infetti non è possibile impostare un'azione di default, in quanto le azioni vengono applicate ad essi a seconda della minaccia rilevata. Se sono presenti più minacce, l'azione appropriata verrà applicata a quella più significativa.

Per configurare le azioni automatiche

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.

3. Attivare l'opzione **Applica le azioni alle minacce automaticamente**.
4. Se necessario, cambiare le azioni automatiche per i tipi di minacce elencati.

Impostazioni aggiuntive

Scansione con privilegi di amministratore

Per eseguire le azioni per alcuni oggetti malevoli, l'applicazione Dr.Web può richiedere i privilegi di amministratore.

Per avviare la scansione con i privilegi di amministratore

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.
3. Premere il pulsante **Avanzate**.
4. Selezionare **Avvia scansione come amministratore**.

Ora prima di ogni scansione il Mac chiederà il nome utente e la password.

È possibile configurare ulteriormente la scansione dei file su richiesta, ossia: includere nella scansione gli archivi e i file di posta, nonché impostare il tempo massimo di scansione di un oggetto.

La modifica di queste impostazioni può portare al rallentamento del Mac e aumentare il tempo di scansione complessivo.

Per attivare la scansione degli archivi e dei file di email

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.
3. Premere il pulsante **Avanzate**.
4. Spuntare i flag **Archivi** e **File di email**.
5. Premere **Salva**.

In modalità **Scansione rapida** gli archivi e i file di posta non vengono controllati.

Per impostare il tempo massimo di scansione di un oggetto

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.
3. Premere il pulsante **Avanzate**.
4. Spuntare il flag **Tempo massimo di controllo di un oggetto**.
5. Impostare il tempo massimo di scansione di un oggetto in secondi.
6. Premere **Salva**.

Risparmio della batteria del Mac

Quando il Mac passa all'alimentazione a batteria, la scansione viene sospesa per rallentare il consumo della carica della batteria. In questo caso Dr.Web chiede all'utente di decidere se continuare o meno la scansione. Al passaggio all'alimentazione da rete elettrica la scansione riprenderà automaticamente.

È possibile disattivare l'opzione di sospensione della scansione al passaggio all'alimentazione a batteria.

Per configurare la scansione all'alimentazione a batteria

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Scanner**.
3. Premere il pulsante **Avanzate**.
4. Disattivare (o attivare) l'opzione **Sospendi la scansione con l'alimentazione a batteria**.
5. Premere **Salva**.

11.2. Esclusione di file e cartelle dalla scansione

È possibile escludere singole cartelle e file dalla scansione su richiesta.

Per escludere file e cartelle dalla scansione

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Eccezioni**.
3. Andare alla scheda **File e cartelle**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.

5. Premere il pulsante + e indicare la cartella o il file da aggiungere alle eccezioni, o trascinare l'oggetto direttamente nella lista delle eccezioni.
6. Premere **Salva**. Ora durante la scansione su richiesta Scanner non controllerà questa cartella o questo file.

Se si vuole annullare temporaneamente l'esclusione di un oggetto dalla scansione, ma lasciarlo nella lista, togliere il flag nella colonna **Scanner** a destra dell'oggetto.

- Per rimuovere un oggetto dalla lista delle eccezioni, selezionarlo nella lista e fare clic su − o trascinare l'oggetto fuori dai confini della finestra dell'applicazione.
- Per ripulire la lista delle eccezioni, selezionare tutti gli elementi nella lista (COMANDO-A) e fare clic su −.

Le impostazioni di eccezioni predefinite sono ottimali per la maggior parte degli usi e non dovrebbero essere modificate senza necessità.

Di default tutte le cartelle di quarantena sono aggiunte alla lista delle eccezioni. Queste cartelle sono progettate per isolare oggetti pericolosi perciò l'accesso ad esse è bloccato e non è necessario controllarle.

12. Protezione della privacy

Dr.Web protegge la privacy dell'utente controllando l'accesso delle applicazioni alla fotocamera e al microfono sul Mac.

Di default l'accesso alla fotocamera e al microfono è consentito a qualsiasi applicazione. È possibile attivare il controllo dell'accesso alla fotocamera e al microfono.

Le impostazioni di controllo dell'accesso alla fotocamera e al microfono sono assenti su macOS 10.14 e versioni successive.

Per attivare il controllo dell'accesso alla fotocamera e al microfono

1. Sulla scheda **Pannello di controllo** della finestra principale selezionare **Protezione della privacy**.
2. Attivare la protezione dell'accesso alla fotocamera o al microfono tramite l'interruttore  .

Ogni volta che un'applicazione cerca di accedere alla fotocamera o al microfono, Dr.Web mostra un avviso e chiede quale azione deve essere utilizzata:

- **Blocca** — vietare all'applicazione l'accesso alla fotocamera o al microfono. L'accesso viene bloccato una volta. A un nuovo tentativo di accesso, per esempio se l'applicazione viene chiusa e riavviata, Dr.Web mostrerà di nuovo l'avviso.
- **Consenti** — consentire all'applicazione l'accesso alla fotocamera o al microfono.

  Per gli utenti dal gruppo Amministratori sono disponibili varianti di controllo accesso aggiuntive:

  - **Consenti una volta** — consentire all'applicazione l'accesso alla fotocamera o al microfono solo una volta.
  - **Consenti sempre** — sempre consentire all'applicazione l'accesso alla fotocamera o al microfono.

  Se è stata selezionata la variante **Consenti sempre**, Dr.Web creerà una regola separata per questa applicazione nella lista delle eccezioni.

  

  Per creare una regola nella lista delle eccezioni, sono richiesti i privilegi di amministratore.

12.1. Consentire l'accesso alla fotocamera e al microfono

È possibile consentire alle singole applicazioni l'accesso alla fotocamera e al microfono.

Le impostazioni di accesso alla fotocamera e al microfono sono assenti su macOS 10.14 e versioni successive.

Per consentire l'accesso alla fotocamere o al microfono

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Eccezioni**.
3. Andare alla scheda **Fotocamera e microfono**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Fare clic su in fondo alla lista **Fotocamera** o **Microfono** e indicare l'applicazione necessaria o trascinarla nella lista corrispondente.

- Per rimuovere un oggetto dalla lista delle eccezioni, selezionarlo nella lista e fare clic su o trascinare l'oggetto fuori dai confini della finestra dell'applicazione.
- Per ripulire la lista delle eccezioni, selezionare tutti gli elementi nella lista (COMANDO-A) e fare clic su .

13. Neutralizzazione delle minacce

13.1. Minacce

Nella sezione **Minacce** è possibile visualizzare la lista completa delle minacce trovate e applicare ad esse le azioni necessarie. Per la neutralizzazione delle minacce configurare le azioni automatiche o applicare manualmente le azioni alle minacce rilevate.

Per visualizzare le informazioni sulle minacce

1. Sulla scheda **Pannello di controllo** della finestra principale premere **Minacce**.

   Sulla scheda **Minacce** sono presentate tutte le minacce rilevate.

   Nella barra di stato nella parte inferiore della finestra vengono mostrati il numero totale di minacce e la loro dimensione complessiva, nonché il numero e la dimensione degli oggetti selezionati.
2. Per visualizzare informazioni su una minaccia, fare clic sul campo corrispondente.
3. Se necessario, è possibile applicare un'azione alla minaccia. Per questo scopo, dalla lista a cascata in fondo alla finestra selezionare:
   - **Rimuovi** — per rimuovere definitivamente l'oggetto dal file system;
   - **Sposta in quarantena** — per mettere l'oggetto in quarantena;
   - **Ignora** — per non eseguire alcuna azione.

Per applicare un'azione a una minaccia

1. Sulla scheda **Pannello di controllo** della finestra principale premere **Minacce**.
2. Selezionare per la minaccia corrispondente un'azione dalla lista a cascata:
   - **Rimuovi** — per rimuovere definitivamente l'oggetto dal file system;
   - **Sposta in quarantena** — per mettere l'oggetto in quarantena;
   - **Ignora** — per non eseguire alcuna azione.
3. Per neutralizzare tutte le minacce rilevate, premere il pulsante **Neutralizza tutto**. Alle minacce verranno applicate le azioni specificate nelle impostazioni dell'applicazione per i tipi di minacce corrispondenti.

Se la lista delle minacce contiene archivi, l'azione viene applicata all'intero archivio nel suo insieme.

Se si vuole applicare l'azione a un file separato, decomprimere l'archivio e avviare nuovamente la scansione.

Per applicare un'azione a più minacce

1. Selezionare più minacce utilizzando il tasto MAIUSCOLE.
2. Utilizzare le specifiche combinazioni di tastii:
   - per rimuovere le minacce, premere COMANDO-MAIUSCOLE-D;
   - per mettere le minacce in quarantena, premere COMANDO-MAIUSCOLE-M.

13.2. Quarantena

Nella sezione **Quarantena** è possibile visualizzare informazioni sugli oggetti che sono stati spostati in quarantena e applicare azioni ad essi. La quarantena è una cartella speciale che consente di isolare le minacce rilevate dal resto del sistema nel caso in cui un oggetto è necessario e non può essere curato.

Per motivi di riservatezza, per ciascun utente viene creata una cartella di quarantena separata. Pertanto, se si è passati alla modalità di utilizzo con privilegi di amministratore, le minacce rilevate verranno spostate nella quarantena dell'amministratore e non saranno disponibili nella quarantena degli utenti.

Per visualizzare informazioni sugli oggetti in quarantena

1. Sulla scheda **Pannello di controllo** della finestra principale premere **Minacce**.
2. Aprire la scheda **Quarantena**.
3. Per visualizzare informazioni su un oggetto in quarantena, fare doppio clic sul campo corrispondente.

Per applicare un'azione a un oggetto in quarantena

1. Sulla scheda **Pannello di controllo** della finestra principale premere **Minacce**.
2. Aprire la scheda **Quarantena**.
3. Selezionare per l'oggetto corrispondente l'azione richiesta dalla lista a cascata:
   - **Rimuovi** — per rimuovere definitivamente l'oggetto dal file system;
   - **Ripristina** — per restituire l'oggetto da quarantena nel percorso da cui è stato spostato;
   - **Ripristina in** — per indicare un percorso per il ripristino dell'oggetto.

Gli oggetti in quarantena non possono essere curati. Se si hanno dubbi che il file sia malevolo, si può controllarlo nuovamente.

È inoltre possibile ripristinare l'oggetto. Gli algoritmi di cura vengono costantemente perfezionati. Probabilmente, l'oggetto potrà essere curato dopo un successivo aggiornamento dell'applicazione.

Se la lista delle minacce contiene archivi, l'azione viene applicata all'intero archivio nel suo insieme.

Se si vuole applicare l'azione a un file separato, decomprimere l'archivio e avviare nuovamente la scansione.

Per applicare un'azione a più minacce

1. Selezionare più minacce utilizzando il tasto MAIUSCOLE.
2. Utilizzare le specifiche combinazioni di tastii:
   - per rimuovere la minaccia, premere COMANDO-MAIUSCOLE-D;
   - per ripristinare l'oggetto nel percorso da cui è stato spostato, premere COMANDO-MAIUSCOLE-R;
   - per indicare un percorso per il ripristino dell'oggetto, premere COMANDO-MAIUSCOLE-P.

14. Supporto

14.1. Guida

Per aprire la guida Dr.Web

1. Nella finestra principale fare clic su .
2. Selezionare la scheda **Aiuto**.

Se le informazioni necessarie non sono state trovate nella guida, consultare la lista delle domande e risposte. Se non è possibile trovare la risposta alla propria domanda e risolvere il problema, contattare il supporto tecnico dell'azienda Doctor Web.

14.2. Domande e risposte

Di seguito sono riportate le descrizioni di alcuni problemi che possono essere riscontrati durante l'utilizzo di Dr.Web, e inoltre sono proposte le possibili soluzioni. Si prega di leggere questa sezione della guida prima di contattare il supporto tecnico.

Problemi generali

Come cambiare la lingua

Il cambio della lingua dell'applicazione è disponibile per gli utenti di macOS 10.15 e versioni successive.

Per cambiare la lingua dell'applicazione

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Selezionare **Generali**.
4. Premere **Lingua e zona**.
5. Premere **App**.
6. Selezionare Dr.Web per macOS e selezionare la lingua dell'applicazione.

I componenti SpIDer Gate, SpIDer Guard e Firewall non si attivano

macOS blocca il caricamento delle estensioni di sistema (moduli del kernel). Per il corretto funzionamento di SpIDer Gate e SpIDer Guard consentire il caricamento del software di sis-

tema Doctor Web Ltd nel pannello **Sicurezza e privacy** nella sezione **Impostazioni di sistema**.

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web Ltd.

Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione prima di poter essere utilizzati** e premere **Dettagli** sotto.
5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa

fare clic sull'icona ⓘ.

7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

La licenza è attivata, ma Dr.Web non funziona

- Probabilmente la licenza è scaduta. Le informazioni sul periodo di validità sono riportate nella sezione **Licenza** della finestra principale Dr.Web  . Se la licenza è scaduta, acquistare una nuova licenza.
- Probabilmente è stato aggiornato il sistema operativo, e la versione Dr.Web installata non supporta la nuova versione macOS. Rimuovere la versione corrente Dr.Web e installare nuovamente l'applicazione.

Dr.Web funziona in modo instabile (si blocca/rallenta)

Ciò può essere causato da un'elevata attività dei processi di sistema che richiedono grandi quantità di memoria operativa. Si consiglia di chiudere le applicazioni non utilizzate in modo da liberare una parte di questa memoria. È possibile visualizzare informazioni sui processi in esecuzione e gestirli tramite l'utility standard macOS Monitoraggio attività.

Se il problema persiste, reinstallare l'applicazione.

Firewall ha bloccato l'accesso a internet

Per l'applicazione che non può ottenere l'accesso a internet creare una regola di permesso nelle impostazioni di Firewall.

Gli avvisi sonori sono configurati ma non funzionano

Controllare il livello del volume nella sezione Preferenze di sistema, nonché sulle casse.

Le impostazioni sono bloccate

Le impostazioni di alcuni componenti sono protette. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su  in fondo alla finestra e inserire il nome utente e la password.

Non funziona il tunnel VPN nell'applicazione AdGuard

Se si riscontrano problemi nell'utilizzo del tunnel VPN di AdGuard, eseguire le seguenti azioni:

1. Aprire le impostazioni AdGuard.
2. Premere **Rete**.
3. Assicurarsi che il flag **Filtra automaticamente il traffico delle app** sia spuntato.
4. Premere **App**.
5. Aggiungere Dr.Web per macOS alla lista delle applicazioni filtrate.

Se non si riesce a trovare Dr.Web per macOS quando si cerca di aggiungerlo alla lista delle applicazioni filtrate, riavviare il Mac e riprovare.

Problemi durante la scansione

La scansione del file system non funziona (impossibile avviare Scanner e/o SplDer Guard)

Probabilmente la licenza è scaduta. Le informazioni sul periodo di validità sono riportate nella sezione **Licenza** della finestra principale Dr.Web  . Se la licenza è scaduta, acquistare una nuova licenza.

I database dei virus impiegano molto tempo per scaricarsi o la scansione avviene lentamente

- Dr.Web scarica i database dei virus all'avvio di una scansione e prima di ciascun tentativo di cura di un oggetto. Quindi, ciò può richiedere un certo tempo.
- Il funzionamento instabile può anche essere causato da un'elevata attività dei processi di sistema che richiedono grandi quantità di memoria operativa. Si consiglia di chiudere le applicazioni non utilizzate in modo da liberare una parte di questa memoria. È possibile visualizzare informazioni sui processi in esecuzione e gestirli tramite l'utility standard macOS Monitoraggio attività.

La scansione salta (non controlla) alcuni file

- Probabilmente i file (o le cartelle in cui sono contenuti) sono esclusi dalla scansione.
- La scansione può saltare alcuni file perché sono danneggiati o protetti da password, e inoltre, se per l'accesso ad essi sono richiesti i privilegi di amministratore. Se nella lista degli oggetti esclusi sono contenuti archivi, decomprimerli prima dell'avvio della scansione.

Scanner si blocca

Se Scanner si è bloccato, chiuderlo e avviarlo nuovamente. Se il problema persiste, reinstallare l'applicazione.

Errore di lettura

Questo errore può verificarsi se Dr.Web non ha l'accesso completo al disco.

Per concedere i permessi per l'accesso completo al disco

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Passare alla sezione **Sicurezza e privacy**.
5. Passare alla sezione **Privacy**.
6. Premere **Accesso al disco**.
7. Aggiungere i moduli Dr.Web alla lista di quelli consentiti.
8. Premere **Riavvia**.

Per macOS 13.0 e versioni successive

1. Nella finestra principale Dr.Web fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Premere **Consenti**.
4. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
5. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando non verrà visualizzata l'icona Dr.Web.
6. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
7. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
8. Premere **Riavvia** per salvare le modifiche.

> Se il pulsante **Consenti** è inattivo, l'accesso al disco è già consentito.

Problemi nel funzionamento di SpIDer Gate

SpIDer Gate non blocca siti secondo le categorie selezionate

- Assicurarsi che nella scheda SpIDer Gate sia spuntato il flag di fronte alla relativa categoria di siti.
- Se la connessione al sito è stata stabilita prima dell'avvio di SpIDer Gate, disattivare e attivare nuovamente SpIDer Gate e quindi riavviare il browser.
- Controllare se il sito utilizza una connessione sicura (generalmente, se la connessione è sicura, nella barra degli indirizzi del browser è visualizzato un lucchetto). Se viene utilizzata una connessione sicura, nella scheda Rete attivare l'opzione **Controlla traffico cifrato** e riavviare il browser.
- SpIDer Gate non blocca siti che utilizzano una connessione attraverso i protocolli FTP/SPDY o HTTP/2.0.

All'apertura di un sito compare un messaggio di errore del certificato

- L'errore può verificarsi perché alcuni browser e client di posta non utilizzano l'archivio certificati di sistema per la ricezione e trasmissione di traffico cifrato. In questo caso installare il certificato dell'azienda Doctor Web che può essere ottenuto tramite il pulsante Esporta sulla scheda Rete.
- Se il browser o client di posta è stato avviato subito dopo l'installazione, poteva non ottenere il certificato di sicurezza di sistema. In questo caso riavviare il browser o client di posta.
- Probabilmente, il certificato del server originale non è affidabile. Per controllare questo, disattivare SpIDer Gate e riavviare il browser o client di posta. Se l'errore persiste, il certificato non è affidabile, e non è consigliato visitare questo sito.

SpIDer Gate ha bloccato un sito necessario

Probabilmente, il sito è incluso in una categoria di siti, l'accesso a cui è bloccato. Per ottenere l'accesso al sito, inserirlo nelle eccezioni.

Aggiornamento

Gli aggiornamenti non vengono scaricati

- Assicurarsi che il Mac sia connesso a internet.

- Se si utilizza un server proxy, disattivarlo e avviare nuovamente l'aggiornamento. Per avviare l'aggiornamento manualmente, nella finestra principale Dr.Web selezionare la voce **Aggiornamento richiesto**.
- Se il router funziona in modalità "Connessione su richiesta", assicurarsi che la connessione sia sempre attiva (cioè il tempo di inattività massimo è di 0 minuti).
- Probabilmente la licenza è scaduta. Le informazioni sul periodo di validità sono riportate nella sezione **Licenza** della finestra principale Dr.Web. Se la licenza è scaduta, acquistare una nuova licenza.

Licenza

La versione di prova non è scaduta, ma la licenza è diventata non valida

- La licenza della versione di prova è legata al checksum del sistema operativo. Probabilmente l'utente ha aggiornato il sistema operativo o altro software o ha sostituito componenti del computer, e quindi il checksum è cambiato.
- La licenza della versione di prova è legata all'indirizzo MAC del dispositivo. Probabilmente l'utente ha cambiato l'indirizzo MAC, e quindi la licenza è diventata non valida.

Contattare il supporto tecnico dell'azienda Doctor Web o attivare una nuova versione di prova utilizzando un altro indirizzo email.

Impossibile attivare la licenza

- Assicurarsi che il Mac sia connesso a internet.
- Se si utilizza un server proxy, disattivarlo e avviare nuovamente l'aggiornamento. Per avviare l'aggiornamento manualmente, nella finestra principale Dr.Web selezionare la voce **Aggiornamento richiesto**.
- Se il router funziona in modalità "Connessione su richiesta", assicurarsi che la connessione sia sempre attiva (cioè il tempo di inattività massimo è di 0 minuti).

Se durante l'utilizzo di Dr.Web si riscontrano problemi la cui soluzione non è descritta sopra, contattare il supporto tecnico dell'azienda Doctor Web. Affinché gli specialisti dell'azienda Doctor Web aiutino il più rapidamente possibile, fornire quante più informazioni possibile sul problema.

14.3. Codici di errore

Codice	Errore	Spiegazione
1	Errore di comunicazione con il monitor	Errore di comunicazione di qualche componente con il daemon di gestione della configurazione Dr.Web ConfigD.
2	L'operazione è già in corso	L'operazione richiesta dall'utente è già in corso.
3	L'operazione è in attesa di esecuzione	L'operazione richiesta dall'utente è al momento in attesa di esecuzione (probabilmente viene stabilita una connessione di rete o vengono effettuati un caricamento e un'inizializzazione di qualche componente del complesso software che richiedono molto tempo).
4	Interrotta dall'utente	L'azione in corso è stata interrotta dall'utente (probabilmente l'esecuzione impiegava troppo tempo).
5	Operazione annullata	L'azione in corso è stata annullata (probabilmente l'esecuzione impiegava troppo tempo).
6	Comunicazione IPC interrotta	La comunicazione IPC con qualche componente del complesso software è stata interrotta (molto probabilmente, il componente ha terminato il suo funzionamento a causa di inattività o in seguito a un comando dell'utente).
7	Dimensioni del messaggio IPC non valide	Durante la comunicazione tra i componenti è stato ricevuto un messaggio di dimensioni non valide.
8	Formato del messaggio IPC non valido	Durante la comunicazione tra i componenti è stato ricevuto un messaggio di formato non valido.
9	Non pronto	L'azione richiesta non può essere eseguita in quanto il componente o dispositivo richiesto non è stato ancora inizializzato.
10	Componente non installato	La funzione richiesta del complesso software Dr.Web non è disponibile in quanto il componente che la realizza non è installato.
11	Messaggio inaspettato IPC	Durante la comunicazione tra i componenti è stato ricevuto un messaggio non valido.
12	Violazioni del protocollo IPC	Durante la comunicazione tra i componenti si è verificata una violazione del protocollo di comunicazione.
13	Stato sottosistema sconosciuto	È stato rilevato che qualche sottosistema del complesso software, richiesto per l'esecuzione dell'operazione, è in uno stato sconosciuto.
20	Il percorso deve essere assoluto	È richiesto il percorso di un file o una directory assoluto (cioè quello che inizia dalla radice del file system), ma è indicato il

Codice	Errore	Spiegazione
		percorso relativo.
21	Memoria insufficiente per completare l'operazione	Memoria insufficiente per eseguire l'operazione richiesta (per esempio, tentativo di decompressione di un file troppo grande).
22	Errore di input/output	Si è verificato un errore di input/output (per esempio, l'unità disco non è stata ancora inizializzata o la partizione del file system non è più disponibile).
23	Nessun file o directory con questo nome	L'oggetto del file system indicato (file o directory) è assente, probabilmente è stato rimosso.
24	Accesso vietato	Permessi insufficienti per accedere all'oggetto del file system indicato (file o directory).
25	Non è una directory	Era aspettato un percorso di directory, ma l'oggetto del file system indicato non è una directory.
26	File di dati danneggiato	I dati a cui è stato effettuato l'accesso sono danneggiati.
27	File esiste già	Al tentativo di creazione del file è stato rilevato che esiste già un file con lo stesso nome.
28	File system di sola lettura	Al tentativo di creazione o modifica dell'oggetto del file system (directory, file o socket) è stato rilevato che il file system è di sola lettura.
29	Errore di rete	Si è verificato un errore di rete (probabilmente l'host remoto ha improvvisamente smesso di rispondere o non è possibile stabilire la connessione richiesta).
30	Non è un'unità disco	Viene effettuato un tentativo di accesso a un'unità di input/output che non è un'unità disco.
31	Fine del file inaspettata	Durante la lettura dei dati è stata inaspettatamente raggiunta la fine del file.
32	Il file è stato modificato	Durante la scansione del file è stato rilevato che era stato modificato.
33	File speciale	Durante l'accesso all'oggetto del file system è stato rilevato che non è un normale file (in altre parole, è una directory, un socket o un altro oggetto del file system).
34	Il nome è già in uso	Al tentativo di creazione dell'oggetto del file system (directory, file o socket) è stato rilevato che esiste già un oggetto con lo stesso nome.
35	Host disconnesso	È stato rilevato che l'host remoto non è disponibile via rete.

Codice	Errore	Spiegazione
36	Raggiunto il limite di utilizzo della risorsa	È stato raggiunto il limite di utilizzo di qualche risorsa.
37	Punti di montaggio diversi	Viene effettuato un tentato di ripristino di un file, che richiede il suo spostamento tra directory di file system appartenenti a punti di montaggio diversi.
38	Errore di decompressione	Non è stato possibile decomprimere l'archivio (probabilmente è protetto da password o danneggiato).
40	Il database dei virus è danneggiato	È stato rilevato che sono danneggiati i database dei virus.
41	Versione dei database dei virus non supportata	È stato rilevato che i database dei virus esistenti sono progettati per una vecchia versione dell'applicazione.
42	Il database dei virus è vuoto	È stato rilevato che i database dei virus sono vuoti.
43	L'oggetto non può essere curato	Un tentativo di applicare l'azione **Cura** a un oggetto incurabile in fase di neutralizzazione della minaccia.
44	Combinazione di database dei virus non supportata	È stato rilevato che il set di database dei virus esistente è incompatibile.
45	Raggiunto il limite di scansione	Durante la scansione dell'oggetto sono state superate le limitazioni impostate (per esempio, quelle alla dimensione del file decompresso, alla profondità dei livelli di nidificazione ecc.).
47	Credenziali utente non valide	Un tentativo di autenticazione con credenziali utente non valide.
48	L'utente non ha i permessi richiesti	Un tentativo di autenticazione con le credenziali di un utente che non ha i permessi richiesti.
49	Token di accesso non valido	Il componente del complesso software ha presentato un token di autenticazione non valido al tentativo di accedere a un'operazione che richiede permessi elevati.
60	Argomento non valido	Al tentativo di esecuzione di qualche comando è stato indicato un argomento non valido.
61	Operazione non valida	È stato effettuato un tentativo di eseguire un comando non valido.
62	Sono richiesti i permessi di superutente	L'azione richiesta può essere eseguita solo da un utente che ha i permessi di superutente.
63	Non è consentito in modalità di protezione centralizzata	L'azione richiesta può essere eseguita solo quando il complesso software funziona in modalità autonoma (standalone).

Codice	Errore	Spiegazione
64	Sistema operativo non supportato	Il sistema operativo installato sull'host non è supportato dal complesso software.
65	Funzione non realizzata	Vengono effettuati tentativi di utilizzare funzioni di qualche componente che non sono realizzate nella versione corrente.
66	Parametro sconosciuto	Il file di configurazione contiene parametri sconosciuti o non supportati nella versione corrente del complesso software.
67	Sezione sconosciuta	Il file di configurazione contiene sezioni sconosciute o non supportate nella versione corrente del complesso software.
68	Valore del parametro non valido	Qualche parametro nel file di configurazione ha un valore non valido per tale parametro.
69	Stato non valido	Qualche componente o tutto il complesso software sono in uno stato non valido ai fini dell'esecuzione dell'operazione richiesta.
70	È consentito un solo valore	Qualche parametro nel file di configurazione ha una lista di valori, il che non è valido per tale parametro.
71	Nome tag non valido	Qualche sezione nel file di configurazione nel cui nome è incluso un tag identificativo univoco ha un valore del tag non valido.
80	Record non trovato	Al tentativo di accedere alle informazioni sulla minaccia trovata è stato rilevato che le informazioni su di essa sono assenti (probabilmente la minaccia è stata già elaborata da un altro componente del complesso software).
81	Record viene attualmente elaborato	Al tentativo di accedere alle informazioni sulla minaccia trovata è stato rilevato che in questo momento viene già elaborata da un altro componente del complesso software.
82	Il file è già in quarantena	Al tentativo di spostare in quarantena il file con la minaccia trovata è stato rilevato che è già in quarantena (probabilmente la minaccia è stata già elaborata da un altro componente del complesso software).
89	Impossibile salvare la copia di backup prima dell'aggiornamento	Prima dell'inizio del download degli aggiornamenti dal server di aggiornamento non è stato possibile salvare la copia di backup dei file da aggiornare.
90	File DRL non valido	È stato rilevato che è danneggiata la struttura di uno dei file delle liste dei server di aggiornamento.
91	File LST non valido	È stato rilevato che è danneggiata la struttura del file contenente la lista dei database dei virus da aggiornare.

Codice	Errore	Spiegazione
92	File compresso non valido	È stato rilevato che è danneggiata la struttura del file caricato contenente gli aggiornamenti.
93	Errore di autenticazione sul server proxy	Non è stato possibile connettersi ai server di aggiornamento attraverso il server proxy definito nelle impostazioni.
94	Nessun server di aggiornamento disponibile	Non è stato possibile connettersi a nessuno dei server di aggiornamento.
95	Formato del file della chiave non valido	È danneggiato il formato del file della chiave.
96	La licenza è scaduta	La licenza esistente è scaduta.
97	Timeout dell'operazione di rete scaduto	Il timeout dell'operazione di rete è scaduto.
98	Checksum non valido	È stato rilevato che è danneggiato il checksum del file caricato contenente gli aggiornamenti.
99	File della chiave di prova non valido	Il file della chiave di prova utilizzato non è valido (per esempio, è stato ottenuto per un altro computer).
100	Il file della chiave di licenza è bloccato	La licenza utilizzata è stata bloccata (probabilmente sono state violate le condizioni del contratto di licenza di uso del prodotto software Dr.Web).
101	Licenza non valida	La licenza utilizzata è progettata per un altro prodotto software o non contiene le autorizzazioni necessarie per il funzionamento dei componenti del prodotto installato.
102	Configurazione non valida	Qualche componente del complesso software non può funzionare a causa di impostazioni di configurazione non valide.
104	File eseguibile non valido	Qualche componente del complesso software non si avvia perché il percorso del suo file eseguibile è indicato in modo errato o il contenuto del file è danneggiato.
105	Motore Virus-Finding Engine non disponibile	È assente o non disponibile il file del motore antivirus Dr.Web Virus-Finding Engine (è richiesto per la ricerca delle minacce).
106	Database dei virus assenti	È stato rilevato che i database dei virus sono assenti.
107	Processo terminato al segnale	Il componente ha terminato il suo funzionamento (probabilmente a causa di inattività o in seguito a un comando dell'utente).
108	Terminazione del processo imprevista	Il componente ha inaspettatamente terminato il suo funzionamento a causa di un malfunzionamento.

Codice	Errore	Spiegazione
109	Software incompatibile rilevato	Il componente del complesso software non può funzionare in quanto è stato rilevato un software che ne impedisce il corretto funzionamento.
112	Database delle categorie di risorse web assenti	È stato rilevato che sono assenti i database delle categorie di risorse web.
113	Modulo di motore per SpIDer Guard non disponibile	Il modulo di motore richiesto per il funzionamento di SpIDer Guard è assente.
117	Componente SpIDer Gate non disponibile	È assente il componente SpIDer Gate (richiesto per la scansione delle connessioni di rete).
118	MailD non disponibile	È assente il componente SpIDer Mail (richiesto per la scansione delle email).
119	Scanning Engine non disponibile	Impossibile controllare i file in quanto è assente o non si avvia il componente Scanning Engine utilizzato per controllare la presenza di contenuti malevoli.
120	Scanner non disponibile	Impossibile controllare i file in quanto è assente il componente Scanner (richiesto per la scansione dei file).
121	ESAgent non disponibile	È assente il componente ESAgent (richiesto per la connessione al server di protezione centralizzata).
122	Componente Firewall non disponibile	Impossibile controllare le connessioni di rete in quanto è assente o non può essere avviato il componente ausiliario Firewall progettato per il reindirizzamento delle connessioni.
123	Network Checker non disponibile	Impossibile controllare le connessioni di rete in quanto è assente o non può essere avviato il modulo ausiliario Network Checker progettato per la scansione dei file scaricati attraverso la rete.
124	Componente CloudD non disponibile	È assente il componente CloudD che è richiesto per l'accesso al servizio Dr.Web Cloud.
125	Errore imprevisto	Si è verificato un errore imprevisto nel funzionamento di qualche componente.

14.4. Supporto tecnico

Se si riscontrano problemi con l'installazione o il funzionamento dei prodotti della società, prima di contattare per l'assistenza il servizio di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

1. Leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/.

2. Leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/.
3. Visitare i forum della società Doctor Web sull'indirizzo https://forum.drweb.com/.

Se provati questi modi, non si è riusciti a risolvere il problema, è possibile utilizzare uno dei seguenti modi per contattare il servizio di supporto tecnico della società Doctor Web:

1. Compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/.
2. Chiamare il numero +7 (495) 789-45-86 o 8-800-333-7932 (numero gratuito per utenti in Russia).

Le informazioni sulle rappresentanze regionali e sedi della società Doctor Web sono ritrovabili sul sito ufficiale sull'indirizzo https://company.drweb.com/contacts/offices/.

15. Impostazioni generali

Nella sezione **Generali** è possibile configurare gli avvisi sonori, gli avvisi visualizzati sullo schermo, ripristinare le impostazioni di default e configurare la registrazione degli eventi nel log per generare un report per il supporto tecnico.

Per modificare le impostazioni generali, non è necessario inserire il nome utente e la password. Le impostazioni cambieranno per tutti gli utenti del Mac automaticamente.

La configurazione degli avvisi in questa sezione del menu è disponibile solo per macOS 10.14 e versioni precedenti. Nelle versioni successive viene effettuata nel menu **Preferenze di sistema** del Mac.

Avvisi

Dr.Web utilizza gli avvisi di sistema macOS per visualizzare messaggi sul rilevamento delle minacce, la loro neutralizzazione o gli errori nel funzionamento dei componenti.

Per disattivare gli avvisi

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Togliere il flag **Attiva avvisi**.

Avvisi sonori

Dr.Web utilizza gli avvisi sonori per informare sul rilevamento di minacce, la loro neutralizzazione e rimozione.

Per disattivare gli avvisi sonori

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Togliere il flag **Utilizza avviso sonoro**.

Ripristino delle impostazioni di default

Se dopo aver modificato le impostazioni si riscontrano problemi nel funzionamento di Dr.Web, ripristinare le impostazioni di default. In questo caso, tutte le modifiche alle im-

postazioni andranno perse.

Per ripristinare le impostazioni di default

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Premere il pulsante **Impostazioni di default**.
5. Premere il pulsante **Ripristina** per confermare il ripristino delle impostazioni dell'applicazione iniziali.

Configurazione della registrazione degli eventi nel log

Affinché sia possibile generare un report sugli eventi per il supporto tecnico, attivare la registrazione degli eventi nel log.

Per attivare la registrazione degli eventi nel log

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Spuntare il flag **Attiva la registrazione degli eventi**.

Questa opzione inoltre consente di assegnare agli eventi dei moduli Dr.Web una classificazione specifica che influenzerà quello quali informazioni verranno rispecchiate nel report sugli eventi.

Per configurare la classificazione degli eventi dei moduli Dr.Web nel log

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Spuntare il flag **Attiva la registrazione degli eventi**.
5. Premere il pulsante **Configurazione**.
6. Selezionare la classificazione richiesta per gli eventi di ciascun modulo.
7. Premere **Salva**.

Nella lista sono disponibili per la configurazione gli eventi dei seguenti moduli e prodotti:

- ConfigD
- SpIDer Guard
- ScanningEngine
- FileCheck
- Firewall
- GateD
- NetCheck
- UrlCheck
- Dr.Web per macOS
- Modulo di aggiornamento
- Agent Dr.Web

Nella tabella seguente sono presentate le possibili varianti di classificazione degli eventi e le relative descrizioni.

Classificazione	Descrizione
DEBUG	La descrizione più dettagliata degli eventi per scopo di debug. Nel report vengono riportati tutti i possibili messaggi che possono aiutare a risolvere il problema.
INFO	Nel report vengono riportati tutti i messaggi, inclusi i messaggi sul normale funzionamento del sistema, l'avvio dei task pianificati, l'avvio e l'arresto dei servizi, sui processi e sulle azioni effettuate dall'utente.
NOTICE	Vengono riportati tutti i messaggi di errore, gli avvertimenti e gli avvisi.
WARNING	Vengono riportati tutti gli avvertimenti e i messaggi di errore.
ERROR	Vengono riportati solo i messaggi di errore.

Configurazione dell'accesso al disco

Per concedere i permessi per l'accesso completo al disco

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic

su  in fondo alla finestra e inserire il nome utente e la password.

4. Passare alla sezione **Sicurezza e privacy**.
5. Passare alla sezione **Privacy**.
6. Premere **Accesso al disco**.
7. Aggiungere i moduli Dr.Web alla lista di quelli consentiti.
8. Premere **Riavvia**.

Per macOS 13.0 e versioni successive

1. Nella finestra principale Dr.Web fare clic su  .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Premere **Consenti**.
4. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
5. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando non verrà visualizzata l'icona Dr.Web.
6. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
7. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
8. Premere **Riavvia** per salvare le modifiche.

 Se il pulsante **Consenti** è inattivo, l'accesso al disco è già consentito.

16. Connessione ai servizi cloud

Dr.Web si connette ai servizi cloud dell'azienda Doctor Web per proteggere il Mac dalle minacce più recenti e migliorare il funzionamento dei componenti dell'applicazione. I servizi cloud aiutano a proteggere gli utenti da file infetti e visite a siti indesiderati.

Le informazioni su minacce, disponibili sul computer, possono diventare obsolete a seconda delle impostazioni di aggiornamento dei database dei virus. L'elaborazione di informazioni nel servizio cloud avviene più velocemente rispetto all'aggiornamento dei database dei virus locali sul computer.

Inoltre, ai server dell'azienda Doctor Web vengono automaticamente inviate informazioni anonime sul funzionamento dei componenti Dr.Web. È possibile leggere l'informativa sulla privacy sul sito ufficiale dell'azienda Doctor Web.

Per disconnettersi dai servizi cloud

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Dr.Web Cloud**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Disattivare l'opzione **Voglio connettermi ai servizi (consigliato)**.

17. Modalità di protezione centralizzata

La protezione centralizzata del Mac viene fornita dall'amministratore del server Dr.Web Enterprise Security Suite o dal provider di servizi internet tramite il servizio antivirus Dr.Web AV-Desk. In questa modalità la licenza personale dell'utente non viene utilizzata.

Impostazioni e componenti

Le impostazioni e il funzionamento dei componenti Dr.Web possono essere modificati o bloccati in conformità ai criteri di sicurezza aziendali o la lista dei servizi pagati del provider. Dal server di protezione centralizzata è possibile controllare:

- Aggiornamento dei database dei virus. Gli aggiornamenti vengono scaricati automaticamente dal server di protezione centralizzata. Se la connessione al server non è disponibile, gli aggiornamenti verranno scaricati tramite internet dai server Dr.Web.
- Protezione del file system continua.
- Scansione del traffico web.
- Scansione antivirus del Mac. L'amministratore della rete antivirus può avviare una scansione remota del Mac dal server manualmente o secondo il calendario.

Connessione del Mac

Ogni Mac con Dr.Web installato è una postazione separata. A seconda delle impostazioni di autenticazione delle postazioni sul server di protezione centralizzata, è possibile connettersi alla rete antivirus:

- Automaticamente, se la postazione è già creata sul server e per essa sono impostati un identificatore e una password.
- Come postazione nuova ("nuovo arrivo"). Dr.Web creerà un nuovo identificatore di postazione e una password. In questo caso potrà essere necessario confermare la postazione sul server, o la postazione verrà autenticata automaticamente con impostazioni di accesso corrispondenti sul server.

> Informazioni sulla connessione delle postazioni al server di protezione antivirus sono disponibili in **Manuale dell'amministratore di Dr.Web Enterprise Security Suite** e **Manuale dell'amministratore di Dr.Web AV-Desk**.

Connessione automatica

Se è stato acquistato un abbonamento al servizio antivirus Dr.Web AV-Desk, è possibile installare Dr.Web tramite un file di formato `.run` che contiene i parametri per la connessione al server. Contattare il provider di servizi internet per ottenere il file `.run`.

Per installare Dr.Web tramite il file .run

1. Rendere eseguibile il file `.run` ottenuto.
2. Avviare il file `.run`.
3. Premere **Installa Dr.Web**.
4. Accettare le condizioni del Contratto di licenza. Inizierà il processo di installazione dell'applicazione.
5. Inserire la password dell'amministratore e premere il pulsante **Installa programma ausiliario**.
6. Alla comparsa dell'avviso **Estensione di sistema bloccata** consentire il caricamento delle estensioni di sistema.
7. Dr.Web verrà copiato nella cartella **Applicazioni** e verrà avviato.
8. Concedere a Dr.Web i permessi per l'accesso completo al disco.

Per rendere il file .run eseguibile

1. Aprire il **Terminale**.
2. Passare alla directory contenente il file .run:

```
cd <tua-directory>
```

3. Inserire il seguente comando:

```
chmod 0755 <nome-file>.run
```

Esempio:

```
cd Desktop
chmod 0755 drweb-12.5.0-av-macosx.run
```

Per consentire il caricamento delle estensioni di sistema

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Passare alla sezione **Sicurezza e privacy**.
4. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
5. Premere **Consenti** accanto al messaggio sul blocco del software di sistema Doctor Web

Ltd.

Per macOS 11.0 e 12.0 premere **Dettagli** e contrassegnare i componenti Dr.Web.

Per macOS 13.0 e 14.0

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Passare alla sezione **Privacy e sicurezza**.
4. In questa sezione trovare la riga **Alcuni software di sistema richiedono la tua attenzione prima di poter essere utilizzati** e premere **Dettagli** sotto.
5. Se le impostazioni non sono disponibili, togliere la protezione. Per fare questo, inserire il nome utente e la password nella finestra a comparsa.
6. Spostare l'interruttore di fronte ai componenti Dr.Web in posizione "on" e premere **OK**.

Per macOS 15.0 e versioni successive

1. Andare al menu Apple .
2. Premere **Impostazioni di sistema**.
3. Andare alla sezione **Generali** e selezionare **Elementi login ed estensioni**.
4. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di sicurezza endpoint** e a destra di essa fare clic sull'icona ⓘ.
5. Spostare l'interruttore **Dr.Web Spider** in posizione "on" e premere **Fine**.
6. Nella sottosezione **Estensioni** trovare la categoria **Estensioni di rete** e a destra di essa fare clic sull'icona ⓘ.
7. Spostare l'interruttore **Dr.Web Firewall** in posizione "on" e premere **Fine**.

Per concedere i permessi per l'accesso completo al disco

Per macOS 12.0 e versioni precedenti

1. Andare al menu Apple .
2. Premere **Preferenze di sistema**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Passare alla sezione **Sicurezza e privacy**.
5. Passare alla sezione **Privacy**.
6. Premere **Accesso al disco**.

7. Aggiungere i moduli Dr.Web alla lista di quelli consentiti.
8. Premere **Riavvia**.

Per macOS 13.0 e versioni successive

1. Nella finestra principale Dr.Web fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Generali**.
3. Premere **Consenti**.
4. Nella Procedura guidata di concessione dell'accesso al disco premere **Vai a Preferenze di sistema**.
5. Nella finestra delle istruzioni della Procedura guidata cliccare sulla freccia fino a quando non verrà visualizzata l'icona Dr.Web.
6. Trascinare l'icona Dr.Web dalla Procedura guidata di concessione dell'accesso al disco e rilasciarla nella finestra delle preferenze di sistema indicata nella Procedura guidata.
7. Per confermare, inserire il nome utente e la password nella finestra a comparsa.
8. Premere **Riavvia** per salvare le modifiche.

Se il pulsante **Consenti** è inattivo, l'accesso al disco è già consentito.

Se l'amministratore della rete antivirus dell'azienda o del provider di servizi internet ha fornito un file di configurazione di formato `.cfg`, è possibile connettere Dr.Web nella sezione **Attivazione della licenza**. I parametri di connessione al server di protezione centralizzata verranno configurati in modo automatico.

Per connettere la postazione tramite il file .cfg

1. Nella finestra principale Dr.Web selezionare la voce **Licenza**.
2. Premere **Attiva**.
3. Nella finestra **Attivazione della licenza** aprire la scheda **File di attivazione**.
4. Trascinare il file di formato `.cfg` nell'area tratteggiata o fare clic per selezionare il file sul Mac.
5. Quando l'attivazione sarà completata, i parametri di connessione al server verranno configurati automaticamente.

Se l'amministratore della rete antivirus dell'azienda ha fornito una chiave di cifratura pubblica di formato `.pub` o un certificato, i parametri di connessione possono essere configurati manualmente.

Per configurare manualmente i parametri di connessione al server

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Modalità**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Attivare l'opzione **Attiva la modalità di protezione centralizzata**. Quando si attiva la modalità centralizzata, vengono ripristinati i parametri dell'ultima connessione.
5. Indicare l'indirizzo IP del server e il numero di porta utilizzato per la connessione al server.
6. Trascinare la chiave di cifratura pubblica di formato `.pub` o il certificato nell'area tratteggiata o fare doppio clic per selezionare il file.
7. Espandere la sottosezione **Autentificazione**.
8. Disattivare l'opzione **Connettiti come nuovo arrivo**. Indicare parametri aggiuntivi per l'autenticazione della postazione:
   - identificatore della postazione;
   - password (assegnata al computer per la registrazione sul server);
   - modalità di compressione del traffico;
   - modalità di cifratura del traffico.

   I valori dei parametri indicati vengono salvati tramite la funzione Keychain. Pertanto, alla riconnessione al server non sarà necessario inserirli nuovamente.
9. Premere **Connettiti**.

Connessione come "nuovo arrivo"

Se l'amministratore non ha ancora creato una postazione sul server, è possibile connettersi come "nuovo arrivo". Contattare l'amministratore della rete antivirus aziendale o il provider di servizi internet per una chiave di cifratura pubblica o un certificato e i parametri di connessione al server di protezione centralizzata.

Per connettere la postazione come "nuovo arrivo"

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Modalità**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Attivare l'opzione **Attiva la modalità di protezione centralizzata**.
5. Indicare l'indirizzo IP del server e il numero di porta utilizzato per la connessione al server.

6. Trascinare la chiave di cifratura pubblica `.pub` o il certificato nell'area tratteggiata o fare doppio clic per selezionare il file.
7. Assicurarsi che nella sottosezione **Autentificazione** sia attivata l'opzione **Connettiti come nuovo arrivo**.
8. Premere **Connettiti**.

Modalità autonoma

È possibile disattivare la modalità di protezione centralizzata e ripristinare il funzionamento autonomo di Dr.Web.

Quando si attiva la modalità di funzionamento autonomo, vengono ripristinate tutte le impostazioni dell'applicazione definite precedentemente al passaggio alla modalità centralizzata, o le impostazioni di default. Inoltre, viene ripreso l'accesso a tutti i componenti Dr.Web.

Per l'utilizzo in modalità autonoma è richiesto un file della chiave valido. La licenza ricevuta automaticamente dal server di protezione centralizzata non può essere utilizzata in questa modalità. Se necessario, attivare una licenza personale.

Per ripristinare la modalità di funzionamento autonomo

1. Nella finestra principale fare clic su .
2. Nella finestra **Preferenze** selezionare la sezione **Modalità**.
3. Se le impostazioni non sono disponibili, togliere la protezione. Per questo scopo fare clic su in fondo alla finestra e inserire il nome utente e la password.
4. Disattivare l'opzione **Attiva la modalità di protezione centralizzata**.
5. Confermare l'azione tramite il pulsante **Disattiva**.

18. Informazioni di guida

18.1. Protezione centralizzata e rete antivirus

Le soluzioni dell'azienda Doctor Web per l'organizzazione della protezione antivirus centralizzata consentono di automatizzare e semplificare la configurazione e la gestione della sicurezza informatica dei computer uniti in un'unica struttura logica (per esempio, computer di un'azienda situati sia dentro che fuori della rete locale). I computer protetti vengono uniti in una *rete antivirus* di cui la sicurezza viene gestita dagli amministratori da un server centrale. La connessione ai sistemi di protezione centralizzata consente di ottenere un livello di protezione del computer garantitamente alto con il minimo sforzo da parte degli utenti finali.

Interazione dei componenti della rete antivirus

Le soluzioni dell'azienda Doctor Web per l'organizzazione della protezione antivirus centralizzata hanno *un'architettura client-server* (v. figura sotto).

I computer di un'azienda o degli utenti di un fornitore di servizi informatici sono protetti dalle minacce alla sicurezza e dallo spam grazie a *componenti* antivirus locali (client; in questo caso — Dr.Web) che assicurano la protezione antivirus e semplificano la connessione al server di protezione centralizzata.

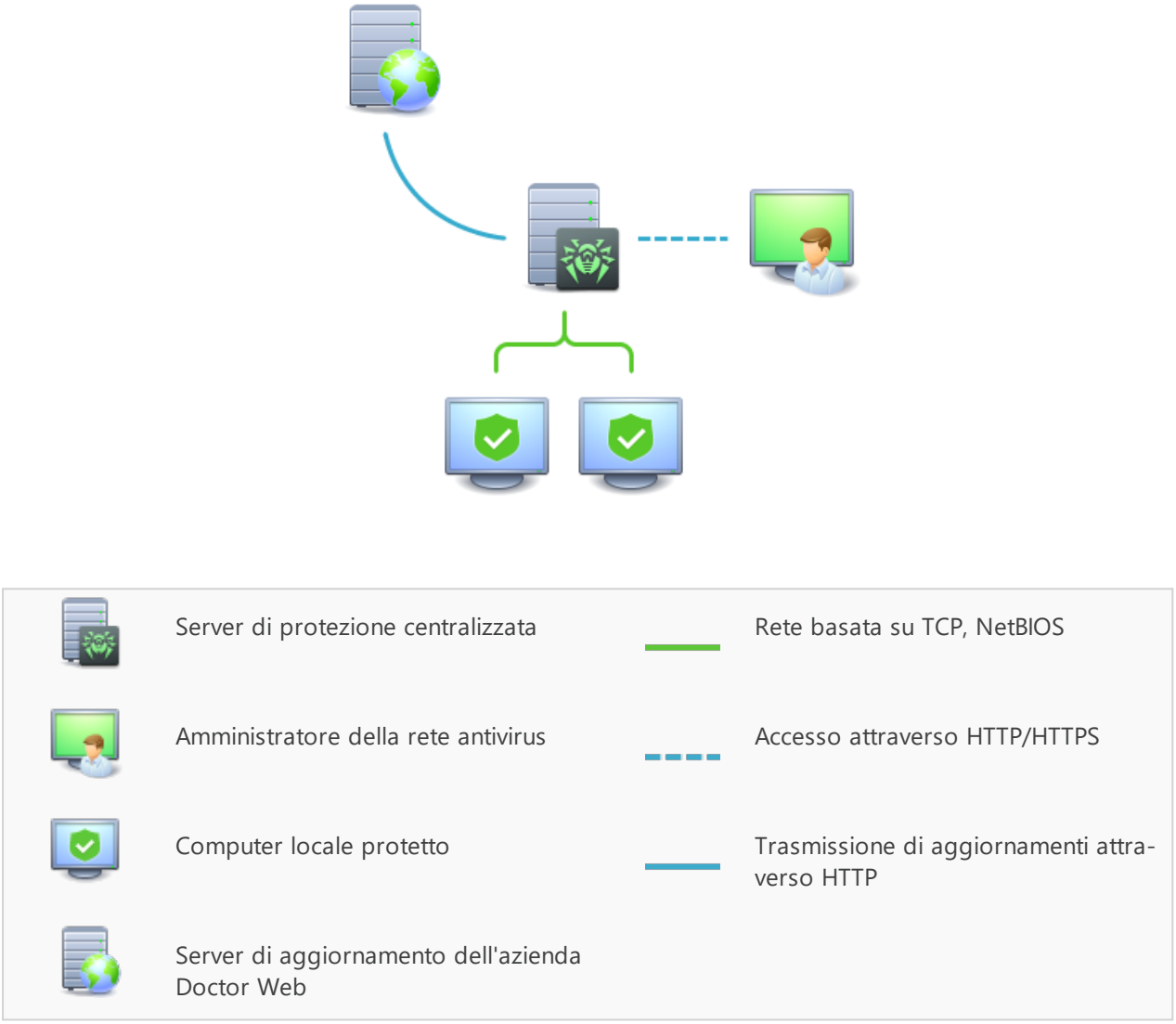

Figura 1. Struttura logica della rete antivirus

L'aggiornamento e la configurazione dei componenti di protezione locali vengono effettuati attraverso il *server centrale*. L'intero flusso di comandi, dati e informazioni statistiche nella rete antivirus anche passa attraverso il server di protezione centralizzata. La quantità di traffico tra i computer protetti e il server antivirus può essere significativa, pertanto, è prevista la possibilità di compressione dati. La cifratura dei dati al trasferimento permette di evitare la fuga di informazioni preziose e la sostituzione furtiva di software caricati su computer protetti.

Tutti gli aggiornamenti necessari vengono caricati sul server di protezione centralizzata dai server di aggiornamento dell'azienda Doctor Web.

La modifica della configurazione dei componenti antivirus locali e la trasmissione dei comandi vengono eseguite dal server antivirus su indicazione degli *amministratori della rete antivirus*. Gli amministratori gestiscono la configurazione del server centrale e la formazione della rete antivirus (in particolare, confermano la legittimità della connessione di una postazione locale alla

rete), e inoltre, se necessario, definiscono le impostazioni di funzionamento di componenti antivirus locali specifici.

> I componenti antivirus locali non sono compatibili né con i software antivirus di altre aziende né con soluzioni antivirus Dr.Web che non supportano la modalità di protezione centralizzata. L'installazione di due programmi antivirus su un singolo computer può portare al blocco del funzionamento del sistema e alla perdita di informazioni importanti.

Soluzioni per la protezione centralizzata

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite è una soluzione antivirus completa per reti aziendali che assicura una protezione affidabile sia delle postazioni che dei file server e server di posta da tutti i tipi di minacce informatiche in aziende di qualsiasi dimensione. Questa soluzione include anche una varietà di strumenti per gli amministratori della rete aziendale che consentono di monitorare i componenti antivirus installati e gestirne il funzionamento, compreso il dispiegamento, l'aggiornamento dei database dei virus Dr.Web e dei moduli software dei componenti, il monitoraggio dello stato della rete, la configurazione degli avvisi di eventi di virus e la raccolta di statistiche.

Servizio internet Dr.Web AV-Desk

Dr.Web AV-Desk è un servizio innovativo dell'azienda Doctor Web per provider di servizi internet. Tramite questo servizio internet i provider possono fornire ai propri utenti (sia privati che aziende) servizi di protezione da virus, spam e altre minacce informatiche. Per usufruire di questi servizi, il cliente dovrà acquistare un abbonamento a qualsiasi pacchetto tariffario per il periodo richiesto. I servizi sono forniti in modalità online.

Informazioni dettagliate sul servizio internet Dr.Web AV-Desk sono disponibili sul sito ufficiale Doctor Web sull'indirizzo https://www.av-desk.com/.

18.2. Tipi di minacce

In questa classificazione il termine "*minaccia informatica*" significa qualsiasi strumento software che sia indirettamente o direttamente capace di causare un danno al computer, alla rete, alle informazioni o ai diritti dell'utente (cioè programmi malevoli e altri programmi indesiderati). In senso più ampio, il termine "minaccia informatica" può significare qualsiasi potenziale pericolo per il computer o la rete (cioè una vulnerabilità che può essere sfruttata per condurre attacchi hacker).

Tutti i tipi di programmi descritti sotto sono potenzialmente capaci di mettere a rischio i dati dell'utente o la loro riservatezza. Di solito, non vengono categorizzati come minacce i pro-

grammi che non nascondono la loro presenza nel sistema (per esempio, alcuni programmi per l'invio dello spam o l'analisi del traffico dati), sebbene in determinate circostanze anch'essi possano causare un danno all'utente.

Virus informatici

Questo tipo di minacce informatiche si distingue per la capacità di incorporare il proprio codice nel codice eseguibile di altri programmi. Tale incorporazione si chiama *infezione*. Nella maggior parte dei casi il file infetto diventa esso stesso portatore del virus, mentre il codice incorporato non necessariamente corrisponde completamente all'originale. La maggior parte dei virus viene creata per danneggiare o distruggere dati.

Nell'azienda Doctor Web i virus sono divisi in base al tipo di file che questi virus infettano:

- *I virus di file* infettano i file del sistema operativo (solitamente file eseguibili e librerie dinamiche) e diventano attivi all'accesso al file infetto.
- *I virus di macro* infettano documenti che vengono utilizzati dai programmi dal pacchetto Microsoft® Office (e da altri programmi che utilizzano macro scritte, per esempio, nel linguaggio Visual Basic). Le *macro* — programmi incorporati, scritti in un linguaggio di programmazione completo che possono avviarsi in determinate condizioni (per esempio, in Microsoft® Word le macro possono avviarsi all'apertura, la chiusura o il salvataggio di un documento).
- *I virus di script* sono scritti nei linguaggi di scripting, e nella maggior parte dei casi infettano altri file di script (per esempio, file di servizio del sistema operativo). Possono infettare anche altri tipi di file che supportano l'esecuzione di script sfruttando gli script vulnerabili nelle applicazioni web.
- *I virus di boot* infettano i settori di avvio di dischi e partizioni, nonché i master boot record dei dischi rigidi. Occupano poca memoria e rimangono pronti per svolgere le loro funzioni fino a quando il sistema operativo non verrà scaricato da memoria, riavviato o arrestato.

La maggior parte dei virus ha meccanismi specifici di protezione contro il rilevamento. I metodi di protezione contro il rilevamento vengono migliorati di continuo, perciò per i programmi antivirus vengono sviluppati nuovi modi per superare questa protezione. I virus possono essere classificati in base al principio di protezione contro il rilevamento:

- *I virus cifrati* a ogni nuova infezione cifrano il proprio codice, il che ne ostacola il rilevamento nel file, nella memoria o nel settore di avvio. Ciascun campione di tale virus contiene solo un breve frammento comune (la procedura di decifratura) che può essere scelto come firma antivirale.
- *I virus polimorfi* utilizzano, oltre alla cifratura del codice, una procedura di decifratura speciale che cambia sé stessa in ogni nuovo campione del virus, il che porta all'assenza di firme antivirali di byte in tale virus.
- *I virus stealth* (virus invisibili) intraprendono azioni speciali per mascherare le loro attività al fine di nascondere la loro presenza negli oggetti infetti. Tale virus ricalca le caratteristiche di un oggetto prima di infettarlo e quindi trasmette i vecchi dati quando arriva una richiesta del sistema operativo o di un programma che cerca file modificati.

Inoltre, i virus possono essere classificati secondo il linguaggio in cui sono scritti (la maggior parte è scritta in linguaggio assembly, ma esistono anche virus scritti in linguaggi di programmazione di altro livello, linguaggi di scripting ecc.), nonché secondo il sistema operativo che viene infettato.

Worm

Recentemente i programmi malevoli di tipo "worm" sono diventati molto più diffusi dei virus e di altri programmi malevoli. Così come i virus, tali programmi sono in grado di creare copie di se stessi, ma non infettano altri oggetti. Un worm si infiltra nel computer dalla rete (il più delle volte come allegato a messaggi di posta elettronica o attraverso internet) e invia le proprie copie funzionali su altri computer. Per iniziare a diffondersi, i worm possono utilizzare sia le attività dell'utente che una modalità automatica di selezione e attacco al computer.

I worm non necessariamente sono costituiti per intero da un singolo file (il corpo del worm). Molti worm hanno una cosiddetta parte infettiva (shellcode) che viene caricata nella memoria operativa del computer e ulteriormente scarica dalla rete il corpo stesso del worm come file eseguibile. Fino a quando il corpo del worm non è arrivato nel sistema, è possibile liberarsi dal worm riavviando il computer (al riavvio la memoria operativa viene resettata). Ma se il corpo del worm è già nel sistema, solo l'antivirus può affrontarlo.

Propagandosi intensamente, i worm possono mettere fuori servizio intere reti anche quando non hanno alcun payload (cioè non causano un danno diretto al sistema).

Nell'azienda Doctor Web i worm sono divisi in base al modo (ambiente) di propagazione:

- *I worm di rete* si diffondono tramite vari protocolli di rete e di condivisione file.
- *I worm di posta* si diffondono tramite protocolli di email (POP3, SMTP ecc.).
- *I worm di chat* si diffondono utilizzando i popolari programmi di messaggistica istantanea (ICQ, IM, IRC ecc.).

Trojan

Questo tipo di programmi malevoli non è in grado di autoreplicarsi. I programmi trojan sostituiscono furtivamente qualche programma frequentemente avviato e ne eseguono le funzioni (o simulano l'esecuzione di tali funzioni) compiendo contemporaneamente attività malevole (danneggiamento e rimozione di dati, trasferimento di informazioni riservate ecc.) o rendendo possibile un uso non autorizzato del computer da parte di un malintenzionato, per esempio, per causare danni a terzi.

Questi programmi hanno funzioni malevole e mimetiche simili a quelle dei virus e persino possono essere un modulo di un virus, ma generalmente i trojan vengono distribuiti come file eseguibili separati (vengono collocati su file server, registrati su supporti di informazione o inviati in email come allegati) che vengono eseguiti dall'utente stesso o da un determinato processo del sistema.

È molto difficile classificare i trojan, primo, perché spesso vengono distribuiti dai virus e worm, secondo, le azioni malevole che possono essere eseguite da altri tipi di minacce solitamente vengono imputate solo ai programmi trojan. Di seguito è riportato un elenco di alcuni tipi di programmi trojan che l'azienda Doctor Web classifica in classi separate:

- *I backdoor* — programmi trojan che consentono di ottenere un accesso privilegiato al sistema aggirando il meccanismo esistente di concessione dell'accesso e di protezione. I backdoor non infettano file; si trascrivono nel registro modificando le chiavi.
- *I rootkit* sono studiati per intercettare le funzioni di sistema del sistema operativo al fine di nascondere la propria presenza nel sistema. Inoltre, i rootkit possono mascherare processi di altri programmi, diverse chiavi del registro, cartelle e file. Un rootkit viene distribuito come programma indipendente o come componente aggiuntivo di un altro programma malevolo. In base al principio di funzionamento, i rootkit sono condizionalmente divisi in due gruppi: quelli che funzionano in modalità utente (intercettano le funzioni delle librerie di modalità utente) *(User Mode Rootkits — UMR)* e quelli che funzionano in modalità kernel (intercettano le funzioni a livello di kernel del sistema, il che rende notevolmente più difficile il rilevamento e la neutralizzazione) *(Kernel Mode Rootkits — KMR)*.
- *I keylogger (software che catturano eventi tastiera*) vengono utilizzati per raccogliere i dati che l'utente inserisce tramite la tastiera. Lo scopo di tali azioni è il furto di informazioni personali (per esempio, password di rete, login, numeri di carte di credito ecc.).
- *I clicker* sostituiscono link che vengono cliccati e in questo modo reindirizzano l'utente su determinati siti web (probabilmente malevoli). Di solito, il reindirizzamento viene effettuato per aumentare il traffico pubblicitario di siti web o organizzare attacchi interruzione distribuita del servizio (attacchi DDoS).
- *I trojan proxy* forniscono al malintenzionato un accesso anonimo a internet attraverso il computer della vittima.

Oltre a quelle elencate, i trojan possono svolgere anche altre funzioni malevole, per esempio cambiare la pagina iniziale nel browser o rimuovere determinati file. Tali azioni però possono essere eseguite anche da altri tipi di minacce (per esempio, virus e worm).

Hacktool

Gli hacktool sono creati con lo scopo di aiutare l'intruso. Il tipo più comune di tali programmi sono gli scanner delle porte che consentono di rilevare le vulnerabilità nei firewall e in altri componenti di protezione del computer. Oltre agli hacker, anche gli amministratori possono utilizzare questi strumenti per testare l'affidabilità delle loro reti. Talvolta vengono classificati come hacktool i programmi che utilizzano metodi di social engineering (ingegneria sociale).

Adware

Il più delle volte, con questo termine si intende il codice software incorporato in vari programmi gratuiti, utilizzando i quali l'utente è costretto a visualizzare pubblicità. Tuttavia, a volte tale codice può diffondersi segretamente attraverso altri programmi malevoli e visualiz-

zare pubblicità, per esempio, nei browser. Spesso gli adware funzionano sulla base dei dati raccolti dai programmi spyware.

Joke

Questo tipo di programmi malevoli, così come gli adware, non causa alcun danno diretto al sistema. Il più delle volte, gli joke generano messaggi su errori inesistenti e minacciano azioni che possono danneggiare dati. La loro funzione principale è quella di intimidire o infastidire l'utente.

Dialer

Sono programmi per computer speciali progettati per scansionare un intervallo di numeri di telefono per trovarne uno su cui risponderà il modem. In seguito, i malintenzionati utilizzano i numeri trovati per aumentare furtivamente il pagamento per il telefono o connettere impercettibilmente l'utente tramite il modem a costosi servizi telefonici.

Riskware

Questi programmi non sono stati creati per causare danni, ma in virtù delle loro caratteristiche, possono rappresentare un rischio per la sicurezza del sistema. A tali programmi appartengono non solo quelli che possono danneggiare o rimuovere accidentalmente i dati, ma anche quelli che possono essere utilizzati dagli hacker o da altri programmi per causare un danno al sistema. Possono essere classificati come riskware diversi programmi di comunicazione e amministrazione remota, server FTP ecc.

Oggetti sospetti

Agli oggetti sospetti appartiene qualsiasi potenziale minaccia rilevata tramite l'analisi euristica. Tali oggetti possono essere qualsiasi tipo di minacce informatiche (probabilmente persino un tipo non conosciuto dagli specialisti di sicurezza informatica) e possono rivelarsi sicuri in caso di falso positivo. Si consiglia di mettere in quarantena i file contenenti oggetti sospetti, nonché inviarli per l'analisi agli specialisti del laboratorio antivirus Doctor Web.

18.3. Metodi di rilevamento delle minacce

Tutti i prodotti antivirus sviluppati da Doctor Web impiegano un intero set di metodi di rilevamento delle minacce, il che consente di verificare oggetti sospetti con la massima accuratezza.

Analisi basata su firme antivirali

Questo metodo di rilevamento viene impiegato in primo luogo. È basato sulla ricerca di firme antivirali delle minacce già conosciute nel contenuto di un oggetto analizzato. La firma anti-

virale è una sequenza di byte continua finita, necessaria e sufficiente per identificare univocamente una minaccia. Il contenuto di un oggetto analizzato viene confrontato con i checksum delle firme antivirali, anziché direttamente con le firme antivirali, il che consente di ridurre notevolmente le dimensioni delle registrazioni nei database dei virus, mantenendo allo stesso tempo l'univocità della corrispondenza e quindi la correttezza del rilevamento delle minacce e della cura degli oggetti infetti. Le registrazioni nei database dei virus Dr.Web sono formate in modo tale che tramite una registrazione sia possibile rilevare intere classi o famiglie di minacce.

Origins Tracing

Questa è una tecnologia unica Dr.Web che consente di rilevare le minacce nuove o modificate di cui il comportamento malevolo o i metodi di infezione sono già conosciuti e descritti nei database dei virus. Viene impiegata dopo l'analisi basata su firme antivirali e protegge gli utenti che utilizzano le soluzioni antivirus Dr.Web dalle minacce quale il trojan ransomware Trojan.Encoder.18 (anche conosciuto come "gpcode"). Inoltre, l'impiego della tecnologia Origins Tracing consente di ridurre notevolmente il numero di falsi positivi nell'analisi euristica. Ai nomi delle minacce rilevate tramite Origins Tracing viene aggiunto il postfisso `.Origin`.

Emulazione dell'esecuzione

Il metodo di emulazione dell'esecuzione del codice software viene utilizzato per rilevare virus polimorfi e cifrati quando la ricerca per checksum delle firme antivirali non può essere impiegata o è notevolmente ostacolata a causa dell'impossibilità di costruire firme affidabili. Il metodo consiste nel simulare l'esecuzione di un codice analizzato tramite un *emulatore* — un modello software del processore e dell'ambiente di esecuzione dei programmi. L'emulatore utilizza una zona di memoria protetta *(buffer di emulazione)*. Le istruzioni non vengono trasferite alla CPU per l'esecuzione effettiva. Se un codice processato dall'emulatore è infetto, il risultato della sua emulazione sarà il ripristino del codice malevolo originale che può quindi essere analizzato tramite l'analisi basata su firme antivirali.

Analisi euristica

L'analisi euristica si basa su un set di *conoscenze euristiche* (ipotesi la cui significatività statistica è stata empiricamente confermata) circa le caratteristiche del codice eseguibile malevolo o, al contrario, sicuro. Ogni caratteristica del codice ha un determinato peso (cioè un numero che indica l'importanza e la validità di tale caratteristica). Il peso può essere sia positivo, se la caratteristica indica la presenza di un comportamento malevolo del codice, che negativo, se la caratteristica non è peculiare delle minacce informatiche. Sulla base del peso complessivo attribuito al contenuto di un oggetto, l'analisi euristica calcola la probabilità di presenza in esso di un oggetto malevolo sconosciuto. Se questa probabilità eccede un determinato valore di soglia, l'analisi euristica conclude che l'oggetto analizzato è malevolo.

L'analisi euristica utilizza, inoltre, la tecnologia FLY-CODE — un algoritmo universale per l'estrazione dei file. Questo meccanismo consente di costruire presupposti euristici sulla

presenza di oggetti malevoli negli oggetti compressi da programmi di archiviazione (packer), non solo quelli conosciuti dagli sviluppatori del prodotto Dr.Web, ma anche quelli nuovi, non ancora studiati. Nel controllo degli oggetti compressi viene anche utilizzata la tecnologia di analisi della loro entropia strutturale che consente di rilevare minacce sulla base delle caratteristiche della posizione dei tratti del loro codice. Questa tecnologia, tramite una sola registrazione del database dei virus, consente di rilevare una serie di varie minacce che sono state compresse da un uguale packer polimorfo.

Siccome l'analisi euristica è un sistema di verifica delle ipotesi in condizioni di incertezza, essa può commettere errori sia del primo tipo (salta minacce sconosciute) e sia del secondo tipo (riconosce come malevolo un programma innocuo). Pertanto, agli oggetti contrassegnati dall'analisi euristica come "malevoli" viene attribuito lo status "sospetti".

Metodo di apprendimento automatico

Viene utilizzato per cercare e neutralizzare oggetti malevoli che ancora non ci sono nei database dei virus. Il vantaggio di questo metodo consiste nel riconoscimento di un codice malevolo senza eseguirlo, solo in base alle sue caratteristiche.

Il rilevamento delle minacce è basato sulla classificazione degli oggetti malevoli secondo determinati segni. Tramite la tecnologia di apprendimento automatico basato sul metodo dei vettori di supporto, frammenti di codice dei linguaggi di scripting vengono classificati e registrati nel database. In seguito gli oggetti di verifica vengono analizzati per conformità ai segni di codice malevolo. La tecnologia di apprendimento automatico automatizza l'aggiornamento della lista di questi segni e l'integrazione dei database dei virus. Grazie alla connessione al servizio cloud, l'elaborazione di grandi quantità di dati avviene più velocemente, mentre l'addestramento continuo del sistema fornisce una protezione preventiva dalle minacce più recenti. La tecnologia può funzionare anche senza connessione costante al cloud.

Il metodo di apprendimento automatico risparmia significativamente le risorse del sistema operativo in quanto non richiede esecuzione di codice per il rilevamento delle minacce, mentre l'addestramento automatico dinamico del classificatore può essere effettuato anche senza un aggiornamento costante dei database dei virus utilizzato nell'analisi basata su firme antivirali.

Tecnologie cloud di rilevamento delle minacce

I metodi di rilevamento cloud consentono di controllare qualsiasi oggetto (file, applicazione, estensione di browser, ecc.) in base alla somma hash. È una sequenza di cifre e lettere univoca di una determinata lunghezza. Nell'analisi in base alla somma hash gli oggetti vengono confrontati con il database esistente e quindi classificati in categorie: pulito, sospetto, malevolo, ecc.

Tale tecnologia ottimizza i tempi di verifica dei file e risparmia risorse del dispositivo. Grazie al fatto che non è l'oggetto stesso che viene analizzato, ma la sua somma hash univoca, la decisione viene presa quasi istantaneamente. In assenza di connessione ai server Dr.Web, i file vengono scansionati localmente, e la verifica cloud viene ripresa al ripristino della connessione.

In questo modo, il servizio cloud dell'azienda Doctor Web raccoglie informazioni da numerosi utenti e aggiorna prontamente i dati su minacce precedentemente sconosciute aumentando così l'efficacia della protezione dei dispositivi.

18.4. Combinazioni tasti

È possibile utilizzare combinazioni di tasti speciali per avviare una scansione, applicare le azioni alle minacce rilevate, nonché per configurare Dr.Web:

Combinazione tasti		**Azione**
Azioni sulle minacce	COMANDO-MAIUSCOLE-C	Cura la minaccia
	COMANDO-MAIUSCOLE-M	Sposta in quarantena la minaccia
	COMANDO-MAIUSCOLE-I	Ignora la minaccia
	COMANDO-MAIUSCOLE-D	Rimuovi la minaccia
	COMANDO-MAIUSCOLE-R	Ripristina la minaccia
	COMANDO-MAIUSCOLE-P	Seleziona la cartella in cui ripristinare la minaccia
Generali	COMANDO-A	Seleziona tutto
	COMANDO-W	Chiudi

© Doctor Web, 2025