



Dr.WEB

Light per Android

Manuale dell'utente



© Doctor Web, 2024. 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 Light per Android
Versione 12.2
Manuale dell'utente
08/05/2024

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. Introduzione	5
1.1. Funzioni di Dr.Web	6
2. Requisiti di sistema	7
3. Installazione di Dr.Web	8
4. Aggiornamento e rimozione di Dr.Web	9
5. Per iniziare	10
5.1. Contratto di licenza	10
5.2. Permessi	10
5.3. Interfaccia	11
5.4. Avvisi	13
5.5. Widget	15
6. Componenti Dr.Web	17
6.1. Protezione antivirus	17
6.1.1. Scanner Dr.Web: scansione su richiesta dell'utente	17
6.1.2. Risultati del controllo	20
6.1.2.1. Minacce nelle applicazioni di sistema	23
6.1.2.2. Modifiche nell'area di sistema	24
6.1.3. Applicazioni che bloccano il dispositivo	25
6.2. Database dei virus	26
6.3. Statistiche	27
6.4. Quarantena	28
6.5. Aiuto all'amico	30
7. Impostazioni	34
7.1. Impostazioni generali	35
7.2. Reset delle impostazioni	36
Indice analitico	37



1. Introduzione

Dr.Web Light protegge i dispositivi mobili con sistema operativo Android™ dalle minacce di virus create appositamente per questi dispositivi.

Nell'applicazione sono utilizzate le progettazioni e tecnologie di Doctor Web per il rilevamento e la neutralizzazione di oggetti malevoli che rappresentano un rischio per la sicurezza informatica del dispositivo e possono influenzare il suo funzionamento.


Dr.Web Light utilizza la tecnologia Origins Tracing™ for Android che trova programmi malevoli per la piattaforma Android. Questa tecnologia consente di individuare nuove famiglie di virus sulla base delle conoscenze sulle minacce già trovate ed esaminate. Origins Tracing™ for Android è in grado di riconoscere sia i virus ricompilati, per esempio Android.SmsSend, Spy che le applicazioni infettate da Android.ADRD, Android.Geinimi, Android.DreamExploid. I nomi delle minacce rilevate tramite Origins Tracing™ for Android hanno l'aspetto «Android.VirusName.origin».

Dr.Web Light utilizza Dr.Web Mobile Engine SDK — insieme di strumenti per la creazione di applicazioni per Android con un elevato livello di sicurezza. Grazie a una varietà di tecniche di rilevamento delle minacce, fornisce protezione dalle minacce per piattaforme mobili, sia conosciute che nuove.

Informazioni sul manuale

Il manuale ha lo scopo di aiutare gli utenti dei dispositivi mobili con sistema operativo Android a installare e configurare l'applicazione, nonché a scoprire le sue funzioni principali.

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
<i>Rete antivirus</i>	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.
Internal storage/Android/	Nomi di file e directory, frammenti di codice.
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a



Simbolo	Commento
	risorse esterne.

1.1. Funzioni di Dr.Web

Dr.Web Light esegue le seguenti funzioni:

- Tiene traccia delle modifiche nel file system del dispositivo in tempo reale (file che vengono salvati, applicazioni che vengono installate ecc.).
- Verifica tutti i file in memoria o singoli file e cartelle a richiesta dell'utente.
- Verifica archivi.
- Tiene traccia delle modifiche nell'area di sistema.
- Rimuove le minacce alla sicurezza rilevate o le sposta in quarantena.
- Sblocca il dispositivo se è stato bloccato da un programma ransomware.
- Aiuta a sbloccare il dispositivo di un amico.
- Aggiorna a cadenza regolare i database dei virus Dr.Web attraverso internet.
- Registra statistiche delle minacce rilevate e delle azioni dell'applicazione e inoltre il log degli eventi.

Dr.Web Light supporta il funzionamento in modalità Multi-Window che consente di avviare più applicazioni in finestre separate. Il funzionamento in questa modalità è possibile solo sui dispositivi Samsung Galaxy S III e versioni successive, Samsung Galaxy Note 2 e versioni successive.



2. Requisiti di sistema

Prima dell'installazione verificare che il dispositivo soddisfi i seguenti requisiti e raccomandazioni:

Parametro	Requisito
Sistema operativo	Android versione 4.4 - 14.0
Processore	x86/x86-64/ARMv7/ARMv8
Memoria operativa libera	Almeno 512 MB
Spazio su disco rigido	Almeno 35 MB (per la conservazione dei dati)
Risoluzione schermo	Risoluzione minima 800×480
Altro	Connessione internet (per l'aggiornamento dei database dei virus)



Su dispositivi con firmware custom o con i permessi di root (i cosiddetti dispositivi rooted) il corretto funzionamento di Dr.Web Light non è garantito.

Di default l'applicazione viene installata nella memoria interna del dispositivo. Per il corretto funzionamento di Dr.Web Light l'applicazione installata non dovrebbe essere trasferita su supporti rimovibili.



3. Installazione di Dr.Web

Installazione da Google Play

Per installare Dr.Web da Google Play, assicurarsi che:

- Si abbia un account Google.
- Il dispositivo sia associato all'account Google.
- Sul dispositivo sia disponibile l'accesso a internet.
- Il dispositivo soddisfi i [requisiti di sistema](#).

Per installare l'applicazione

1. Aprire Google Play sul dispositivo, trovare Dr.Web Light nella lista delle applicazioni e premere il pulsante **Installa**.



Se Dr.Web Light non viene visualizzato in Google Play, il dispositivo non soddisfa i [requisiti di sistema](#).

2. Per iniziare a usare l'applicazione, premere il pulsante **Apri**.

Installazione da Xiaomi GetApps

Per installare Dr.Web da Xiaomi GetApps, assicurarsi che:

- Si abbia un account Xiaomi.
- Il dispositivo sia associato all'account Xiaomi.
- Sul dispositivo sia disponibile l'accesso a internet.
- Il dispositivo soddisfi i [requisiti di sistema](#).

Per installare l'applicazione

1. Aprire Xiaomi GetApps sul dispositivo, trovare Dr.Web Light nella lista delle applicazioni e premere il pulsante **Ottieni**.



Se Dr.Web Light non viene visualizzato in Xiaomi GetApps, il dispositivo non soddisfa i [requisiti di sistema](#).


2. Per iniziare a usare l'applicazione, premere il pulsante **Apri**.



4. Aggiornamento e rimozione di Dr.Web

Aggiornamento di Dr.Web

Se per le applicazioni da Google Play non è configurato l'aggiornamento automatico, è possibile avviare l'aggiornamento in maniera manuale:

1. Aprire l'applicazione **Play Store**.
2. Premere l'icona del proprio profilo Google.
3. Selezionare la voce **Gestisci app e dispositivo**.
4. Passare alla scheda **Gestisci**.
5. Premere la lista **Aggiornamenti disponibili** ed eseguire una delle azioni:
 - Selezionare **Dr.Web Light** e premere **Aggiorna**.
 - Spuntare il flag di fronte a **Dr.Web Light** e premere l'icona .



L'applicazione si trova nella lista **Aggiornamenti disponibili** se è già stata rilasciata una nuova versione dell'applicazione.

6. Quando viene aggiornata, l'applicazione potrebbe richiedere nuovi permessi. In questo caso si aprirà una finestra per la conferma.

Premere il pulsante **Accetta** per consentire l'accesso alle funzioni del dispositivo necessarie per l'applicazione.

Per iniziare a usare l'applicazione, premere il pulsante **Apri**.

Rimozione di Dr.Web

Per rimuovere Dr.Web

1. Nelle impostazioni del dispositivo selezionare **Applicazioni** o **Gestione delle applicazioni**.
2. Nell'elenco delle applicazioni installate selezionare **Dr.Web Light** e premere **Elimina**.

La cartella quarantena e i file di log non vengono rimossi in maniera automatica. È possibile rimuoverli manualmente dalla cartella `Android/data/com.drweb/files` nella memoria interna del dispositivo.



Sui dispositivi con Android 11 e versioni successive i log vengono salvati nella cartella `Download/DrWeb`.



5. Per iniziare

Dopo l'installazione di Dr.Web Light è possibile familiarizzare con l'interfaccia e il menu principale dell'applicazione, configurare la barra delle notifiche e impostare un widget di Dr.Web sulla schermata principale del dispositivo.

5.1. Contratto di licenza

Al primo avvio dell'applicazione si aprirà il Contratto di licenza che l'utente deve accettare per continuare a utilizzare l'applicazione.

Sulla stessa schermata viene chiesto di accettare la clausola sull'invio delle statistiche di funzionamento dell'applicazione e di minacce trovate sui server Doctor Web, nonché sui server Google e Yandex. La possibilità di rifiutarsi di inviare le statistiche esiste nella versione estesa di Dr.Web.

5.2. Permessi

A partire dalla versione 6.0 nel sistema operativo Android è comparsa la possibilità di consentire o vietare alle applicazioni l'accesso alle funzioni del dispositivo e ai dati personali.

Dopo aver installato Dr.Web Light e accettato il Contratto di licenza, concedere all'applicazione i permessi necessari. Dr.Web Light chiede i seguenti permessi obbligatori:

- Sui dispositivi con Android 10.0 o versioni precedenti: l'accesso a foto, contenuti multimediali e file.
- Sui dispositivi con Android 11.0 o versioni successive: l'accesso a tutti i file.

Senza concedere i permessi obbligatori, l'utilizzo di Dr.Web Light non è possibile. La richiesta dei permessi verrà visualizzata ogni volta che si accede all'applicazione fino a quando non si concederanno i permessi secondo le istruzioni riportate di seguito o visualizzate sulla schermata della richiesta.

Sui dispositivi con Android 13.0 o versioni successive Dr.Web Light chiede il permesso di invio delle [notifiche](#). Il permesso è richiesto affinché Dr.Web Light possa utilizzare la barra delle notifiche per i messaggi di stato di protezione del dispositivo. Se il permesso non verrà concesso, Dr.Web Light non potrà informare l'utente sul rilevamento di minacce e sulla necessità di controllo di file sospetti fino a quando l'applicazione non verrà aperta.


Se l'utente rifiuta la richiesta di concessione dei permessi obbligatori, gli verrà chiesto di passare alla schermata delle impostazioni:

- Sui dispositivi con Android 9.0 o versioni precedenti:
 1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.



2. Selezionare la voce **Memoria** o **Archiviazione** e concedere il permesso utilizzando l'interruttore.
- Sui dispositivi con Android 10.0:
 1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.
 2. Selezionare la voce **Memoria** o **Archiviazione** nella categoria **Rifiutate** e selezionare l'opzione **Consenti**.
 - Sui dispositivi con Android 11.0 o versioni successive:
 1. Premere **Vai su Impostazioni** e selezionare la sezione **Permessi**.
 2. Selezionare la voce **File e contenuti multimediali** o **Archiviazione** nella categoria **Rifiutate** e selezionare l'opzione **Consenti la gestione di tutti i file**. Tramite questa opzione viene concesso l'accesso a foto e contenuti multimediali, nonché l'accesso a tutti i file.

Per aprire la lista di tutti i permessi per Dr.Web Light

1. Aprire le impostazioni del dispositivo .
2. Premere **Applicazioni** o **Gestione delle applicazioni**.
3. Trovare nella lista delle applicazioni installate Dr.Web Light e premerlo.
4. Nella schermata **Informazioni applicazione** selezionare la voce **Permessi**.
5. Nel menu locato nell'angolo superiore destro selezionare **Tutti i permessi**.

5.3. Interfaccia

Schermata principale

Al primo accesso all'applicazione si trovano sullo schermo una barra di stato, informazioni sulla versione completa dell'applicazione, il [menu di Scanner Dr.Web](#), nonché la barra di navigazione Dr.Web (vedi [Immagine 1](#)).

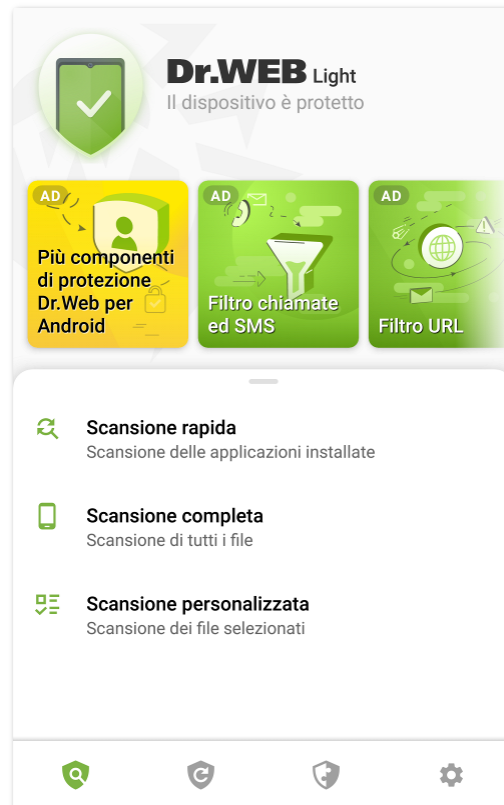


Immagine 1. Schermata principale Dr.Web

Barra di stato

Nella parte superiore della schermata principale Dr.Web si trova una barra di stato con un indicatore che mostra lo stato corrente della protezione del dispositivo (vedi [Immagine 2](#)).



Immagine 2. Barra di stato

- L'indicatore verde significa che il dispositivo è protetto. Non è richiesta alcuna azione aggiuntiva.
- L'indicatore giallo significa che Dr.Web ha rilevato problemi di sicurezza, per esempio, nuovi file sono stati aggiunti sul dispositivo o i database dei virus non sono aggiornati. Premere la barra per avviare una [scansione personalizzata](#) del dispositivo.







Informazioni sulla versione completa dell'applicazione

Sotto la barra di stato sono situate slide sulle funzionalità della versione completa dell'applicazione. Le slide consentono di visualizzare informazioni sull'antivirus Dr.Web Security Space per Android e scaricarlo da Google Play.

Premere la prima slide per aprire la pagina Dr.Web Security Space per Android su Google Play. Premere qualsiasi delle seguenti slide per scoprire le funzionalità di uno dei componenti disponibili in Dr.Web Security Space per Android. Il pulsante **Più nel dettaglio** sulla slide consente di aprire la pagina Dr.Web Security Space per Android sul sito dell'azienda Doctor Web. Far scorrere il dito con la slide verso sinistra per passare alla slide successiva.

Barra di navigazione

Nella parte inferiore dello schermo è situata la barra di navigazione Dr.Web attraverso cui è possibile passare da una scheda di componente a un'altra.

- La scheda  [Scanner](#) consente di avviare una scansione del sistema su richiesta dell'utente. Sono possibili 3 tipi di scansione: rapida, completa e personalizzata.
- La scheda  [Database dei virus](#) informa sullo stato corrente dei database dei virus e consente di avviare manualmente l'aggiornamento dei database dei virus.
- La scheda  **Strumenti** include i seguenti componenti:
 - [Statistiche](#) consente di visualizzare le statistiche delle minacce rilevate e delle azioni eseguite dall'applicazione su di esse.
 - [Quarantena](#) consente di visualizzare ed elaborare le minacce spostate in quarantena.
 - [Aiuto all'amico](#) aiuta a sbloccare il dispositivo di un amico che è bloccato da Antifurto Dr.Web.
- La scheda  [Impostazioni](#) consente di gestire le impostazioni dei componenti e dell'applicazione Dr.Web.

5.4. Avvisi

Sui dispositivi con Android 7.0 o versioni successive tutti gli avvisi Dr.Web vengono raggruppati in un unico avviso a tendina.

Sui dispositivi con Android 8.0 o versioni successive gli avvisi Dr.Web sono suddivisi in categorie, o canali. Nelle impostazioni del dispositivo è possibile gestire separatamente il comportamento di ciascuna categoria di avvisi. Se si disattiva una delle categorie, non si riceverà più avvisi da questa categoria. Di default tutte le categorie sono attivate.



Categorie di avvisi

Categoria	Avvisi
Rilevamento di una minaccia	Avvisi di minacce rilevate da Scanner Dr.Web.
Stato della protezione antivirus	Se la barra delle notifiche è disattivata, questa categoria contiene i seguenti avvisi: <ul style="list-style-type: none">• Il dispositivo è protetto. Viene visualizzato se la scansione di Scanner Dr.Web non è in esecuzione.• Avviso di tipo di scansione di Scanner Dr.Web. Viene visualizzato se è in esecuzione una delle scansioni: rapida, completa o personalizzata. Se la barra delle notifiche è attivata, su di essa viene visualizzato un messaggio di scansione in corso, se una delle scansioni di Scanner Dr.Web è in esecuzione.
Avvisi dagli amici	Avvisi ricevuti dagli amici.
Altro	<ul style="list-style-type: none">• Sono richieste autorizzazioni. Viene visualizzato all'apertura dell'applicazione se la richiesta di accesso a foto, file multimediali e altri è stata precedentemente rifiutata.
Raggruppa avvisi	Questa categoria non contiene avvisi specifici, ma consente di raggruppare tutti gli avvisi Dr.Web in un unico avviso a tendina.

Barra delle notifiche

La barra delle notifiche Dr.Web (vedi [Immagine 3](#)) visualizza prontamente gli avvertimenti di modifiche sospette nell'area di sistema e quelli di minacce.

Nella barra delle notifiche Dr.Web viene visualizzato un indicatore di stato di protezione

corrente:  — sui dispositivi con Android 11.0 e versioni precedenti,  — sui dispositivi con Android 12.0 e versioni successive. Se Dr.Web rileverà nuovi file sul dispositivo o modifiche sospette nell'area di sistema, il colore dell'indicatore cambierà in giallo. Se Dr.Web rileverà minacce, il colore dell'indicatore cambierà in rosso.

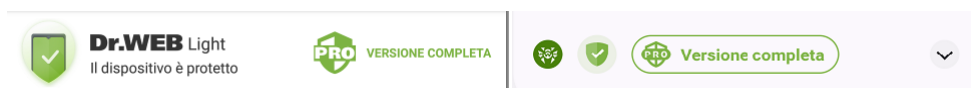



Immagine 3. Barra delle notifiche su Android 11.0 (a sinistra) e Android 12.0 (a destra)

Per attivare la barra delle notifiche Dr.Web

1. Premere l'icona  sulla barra di navigazione Dr.Web.
2. Selezionare **Impostazioni generali**.



3. Attivare l'opzione **Barra delle notifiche**.



Su Android 5.0 e 5.1, se Dr.Web rileverà modifiche sospette nell'area di sistema o minacce, la barra delle notifiche viene visualizzata sopra tutte le applicazioni fino a quando un'azione non verrà applicata all'oggetto rilevato o l'avviso non verrà cancellato dalla barra delle notifiche.

Tramite la barra delle notifiche è possibile eseguire le seguenti azioni:

- Aprire la [schermata principale](#) dell'applicazione in caso di indicatore verde e stato di protezione corrente **Il dispositivo è protetto**. Per farlo, premere l'indicatore.
- Avviare la [scansione personalizzata](#) in caso di indicatore giallo e stato di protezione corrente **Avviare scansione**. Per farlo, premere l'indicatore.
- Aprire i [risultati della scansione](#) in caso di indicatore rosso e stato di protezione corrente **Risolvere i problemi**. Per farlo, premere l'indicatore.
- Conoscere informazioni sull'applicazione Dr.Web Security Space per Android e scaricarla per un periodo gratuito di 14 giorni. Per farlo, premere il testo **Versione completa**.

Per visualizzare lo stato di protezione, le azioni correnti e quelle consigliate sui dispositivi con Android 12.0 e versioni successive, premere ▼.

5.5. Widget

Per la comodità dell'utilizzo di Dr.Web Light è possibile aggiungere alla schermata principale del dispositivo uno specifico widget che permette di monitorare lo stato di protezione del dispositivo.

Per aggiungere il widget Dr.Web

1. Aprire la lista dei widget disponibili sul dispositivo.
2. In questa lista selezionare il widget Dr.Web.

Il widget mostra lo stato di protezione corrente (vedi [Immagine 4](#)).

- Un widget senza indicatore informa sull'assenza di minacce. Non è richiesta alcuna azione aggiuntiva.
- Un widget con un indicatore giallo informa sul rilevamento di nuovi file o applicazioni sul dispositivo. Premere il widget per avviare la scansione dei nuovi oggetti.
- Un widget con un indicatore rosso informa sulla necessità di neutralizzare le minacce rilevate. Premere il widget per aprire la schermata dei risultati della scansione e selezionare le azioni per le minacce rilevate.

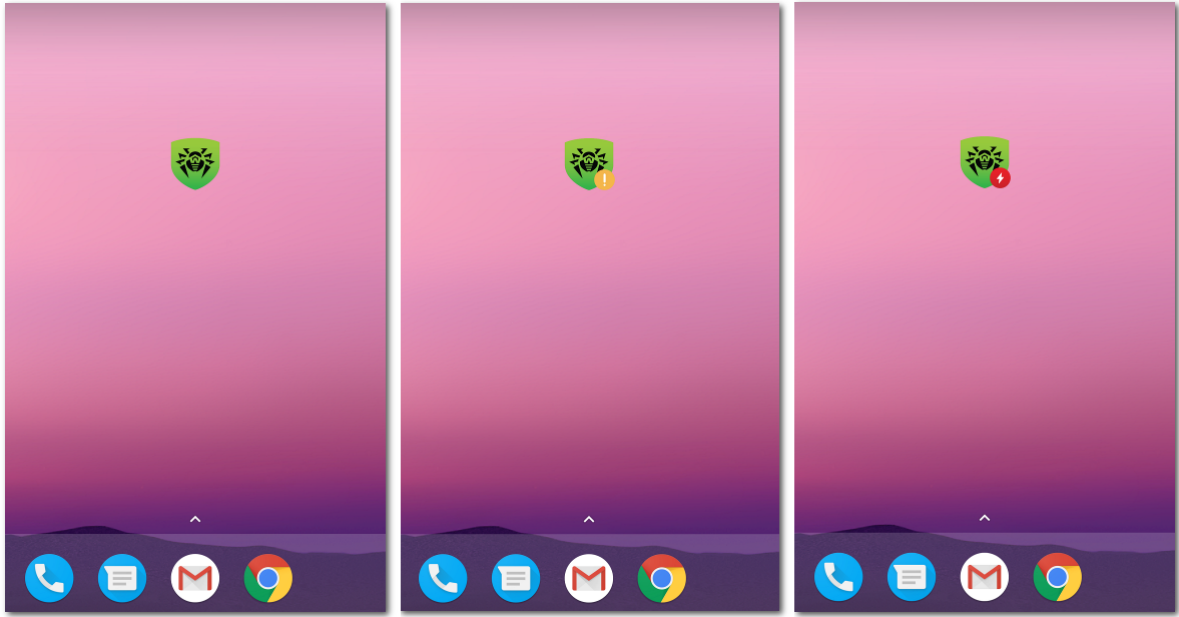








Immagine 4. Widget Dr.Web



6. Componenti Dr.Web

È possibile passare a un componente Dr.Web tramite la [barra di navigazione](#) nella parte inferiore dello schermo.

-  [Scanner](#): consente di avviare una scansione del sistema su richiesta dell'utente. Sono possibili 3 tipi di scansione: rapida, completa e personalizzata.
-  [Database dei virus](#): informa sullo stato corrente dei database dei virus e consente di avviare manualmente l'aggiornamento dei database dei virus.
-  [Statistiche](#): consente di visualizzare le statistiche delle minacce rilevate e delle azioni eseguite dall'applicazione su di esse.
-  [Quarantena](#): consente di visualizzare ed elaborare le minacce spostate in quarantena.
-  [Aiuto all'amico](#): aiuta a sbloccare il dispositivo di un amico che è bloccato da Antifurto Dr.Web.
-  [Impostazioni](#): consente di gestire le impostazioni dei componenti e dell'applicazione Dr.Web.

6.1. Protezione antivirus

- [Scanner Dr.Web](#) consente di avviare una scansione per controllare la presenza di minacce.
- Sulla schermata [Risultati del controllo](#) è possibile selezionare le azioni per neutralizzare le minacce alla sicurezza rilevate.

6.1.1. Scanner Dr.Web: scansione su richiesta dell'utente

La scansione del sistema su richiesta dell'utente viene eseguita dal componente Scanner Dr.Web. Consente di eseguire la scansione rapida o completa del file system, nonché controllare singoli file e cartelle.

Si consiglia di eseguire periodicamente la scansione del file system. Di solito in tale caso è sufficiente eseguire la scansione rapida del sistema.

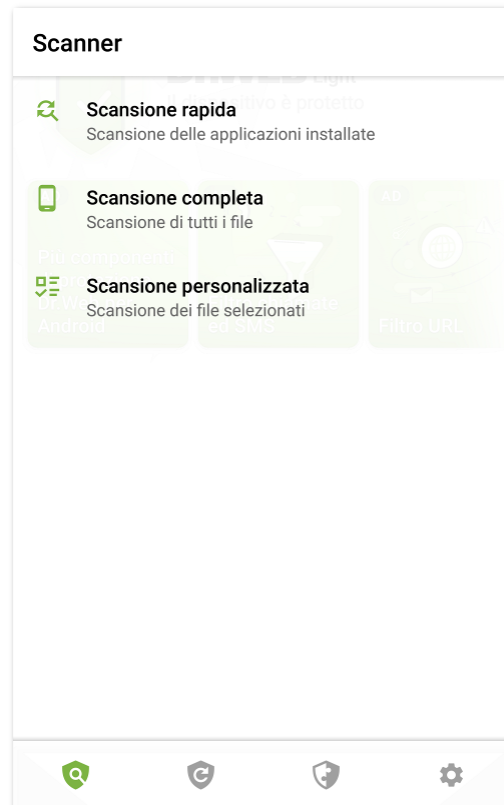



Immagine 5. Scanner Dr.Web

Scansione

Per eseguire una scansione del sistema, sulla barra di navigazione Dr.Web premere l'icona , quindi sulla schermata **Scanner** (vedi [Immagine 5](#)) eseguire una delle seguenti azioni:

- Per avviare una scansione delle sole applicazioni installate, selezionare la voce **Scansione rapida**.
- Per avviare una scansione di tutti i file, selezionare la voce **Scansione completa**.
- Per controllare singoli file e cartelle, selezionare la voce **Scansione personalizzata**, quindi selezionare gli oggetti richiesti nella lista comparsa degli oggetti del file system (vedi [Immagine 6](#)). Per selezionare tutti gli oggetti, spuntare la casella nell'angolo superiore destro dello schermo. Quindi premere **Controlla**.



Sui dispositivi con Android 11.0 e versioni successive, le cartelle `/Android/data` e `/Android/obb` sono protette dal sistema e non sono disponibili per la scansione.

Se durante qualsiasi scansione Scanner Dr.Web rileverà minacce, l'indicatore al centro della schermata di scansione diventerà rosso. Premere l'indicatore o il numero di minacce trovate per aprire i risultati della scansione (vedi [Immagine 7](#)) e [neutralizzare le minacce](#). Se è stata chiusa la schermata di scansione o è stata chiusa l'applicazione, è possibile aprire i risultati della scansione premendo l'icona sulla [barra delle notifiche](#).

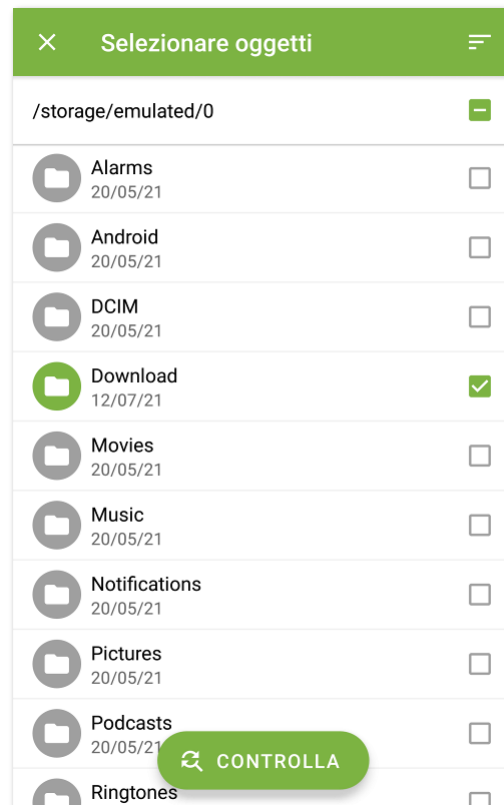


Immagine 6. Scansione personalizzata

Invio di file sospetti al laboratorio antivirus Doctor Web

È possibile inviare al laboratorio antivirus Doctor Web archivi ZIP sospetti (file con l'estensione .jar, .apk) che presumibilmente contengono virus, file con l'estensione .odex, .dex, .so, o archivi ZIP sicuramente puliti che provocano il cosiddetto falso positivo.

Per inviare un file al laboratorio

1. Premere e tenere premuto un file nella lista degli oggetti del file system (vedi [Immagine 6](#)), quindi premere il pulsante **Invia al laboratorio**.
2. Sulla schermata successiva immettere un indirizzo email se si desidera ricevere i risultati dell'analisi del file inviato.
3. Scegliere una delle categorie di richiesta:
 - **Probabile virus**, se si ritiene che il file sia una minaccia.
 - **Falso positivo**, se si ritiene che il file sia erroneamente classificato come minaccia.
4. Premere il pulsante **Invia**.



Al laboratorio antivirus Doctor Web è possibile inviare file di cui le dimensioni non superano 250 MB.

Impostazioni di Scanner Dr.Web

Per accedere alle impostazioni di Scanner Dr.Web, passare alla schermata [Impostazioni](#) e selezionare la voce **Scanner**.

- Per attivare il controllo di file in archivi compressi, spuntare il flag **File in archivi**.



Di default il controllo di archivi è disattivato. L'attivazione del controllo di archivi può influire sulle prestazioni del sistema e aumentare il consumo della batteria. La disattivazione del controllo di archivi non influisce sul livello di protezione in quanto Scanner Dr.Web controlla i file APK di installazione indipendentemente dal valore impostato del parametro **File in archivi**.




- Per monitorare le [modifiche nell'area di sistema](#), spuntare i flag **Area di sistema** e **Qualsiasi file dell'area di sistema**. Se queste impostazioni sono attivate, il componente monitora le modifiche (aggiunta, modifica e rimozione di file) e avvisa dell'aggiunta e della modifica di file eseguibili: `.jar`, `.odex`, `.so`, file di formato APK, ELF, ecc.
- Per attivare/disattivare il controllo della presenza nel sistema di file che possono rappresentare una minaccia, spuntare/togliere i flag corrispondenti:
 - Oggetti sospetti,
 - Programmi adware,
 - Programmi dialer,
 - Programmi joke,
 - Riskware,
 - Programmi hacktool,
 - Programmi vulnerabili.

Statistiche

L'applicazione registra gli eventi relativi al funzionamento di Scanner Dr.Web (tipo di scansione, risultati della scansione, rilevamento di minacce alla sicurezza). Le azioni dell'applicazione vengono visualizzate nella sezione **Eventi** nella scheda **Statistiche**, ordinate per data (vedi sezione [Statistiche](#)).

6.1.2. Risultati del controllo

Se Scanner Dr.Web rileverà minacce, sulla schermata appariranno:

- Un'icona nella barra di stato di Android nell'angolo superiore sinistro dello schermo:
 -  — su Android 4.4,
 -  — su Android 5.0–11.0,
 -  — su Android 12.0 e versioni successive.



- Un avviso a comparsa nella parte superiore dello schermo.
- Un indicatore rosso sulla schermata di controllo.

Per aprire i risultati del controllo, premere la croce nell'angolo superiore sinistro della schermata di scansione completata o l'indicatore nell'avviso o nella barra di stato.



Su Android 5.0 e versioni successive l'avviso di minaccia compare anche sulla schermata di blocco del dispositivo da cui è possibile passare ai risultati del controllo.

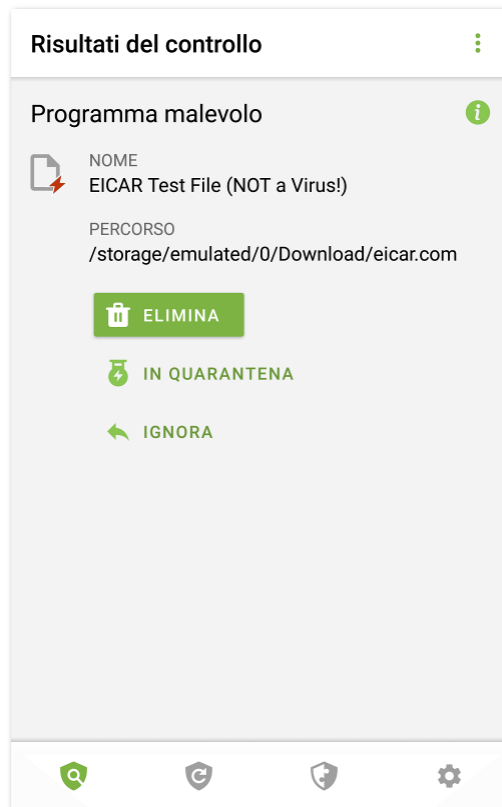


Immagine 7. Risultati del controllo

Neutralizzazione delle minacce

Sulla schermata **Risultati del controllo** è possibile visualizzare la lista delle minacce e delle modifiche sospette nell'area di sistema. Per ciascun oggetto sono indicati il suo tipo e nome.

Gli oggetti sono contrassegnati con colori diversi a seconda del grado di pericolo. Tipi di oggetti in ordine di diminuzione del pericolo:

1. Programma malevolo.
2. Variante. Sulla schermata **Risultati del controllo** il tipo di oggetto è visualizzato come **Programma malevolo**, ma l'indicazione di colore differisce.



3. Oggetto sospetto.
4. Programma adware.
5. Programma dialer.
6. Joke.
7. Riskware.
8. Hacktool.
9. Programma vulnerabile.

Il grado di pericolo più basso viene attribuito alle [modifiche nell'area di sistema](#):

- File nuovi nell'area di sistema.
- Modifica dei file di sistema.
- Eliminazione dei file di sistema.

Per visualizzare il percorso di un file, selezionare l'oggetto corrispondente. Nel caso di minacce rilevate in applicazioni è indicato anche il nome del pacchetto dell'applicazione.

Se viene rilevato un archivio contenente più minacce, selezionare l'oggetto corrispondente e premere **Espandi** per espandere la lista completa di tutte le minacce nell'archivio.



Il rilevamento di minacce in archivi è possibile solo se è attivata l'opzione [File in archivi](#).

Neutralizzazione di tutte le minacce

Per rimuovere tutte le minacce contemporaneamente


- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu**  > **Elimina tutto**.

Per spostare in quarantena tutte le minacce contemporaneamente

- Nell'angolo superiore destro della schermata **Risultati del controllo** selezionare **Menu**  > **Tutto in quarantena**.

Neutralizzazione delle minacce una per una

Per ciascun oggetto è disponibile il proprio set di opzioni. Per espandere una lista delle opzioni, selezionare un oggetto. Le opzioni consigliate sono elencate per prime. Selezionare una delle opzioni:

 **Elimina** per rimuovere completamente una minaccia dalla memoria del dispositivo.

In alcuni casi Dr.Web non può rimuovere applicazioni che utilizzano le funzioni accessibilità



Android. Se Dr.Web non rimuoverà un'applicazione dopo che viene selezionata l'opzione **Elimina**, passare a modalità provvisoria e disinstallare manualmente l'applicazione.

L'opzione non è disponibile per le [minacce nelle applicazioni di sistema](#).



In quarantena per spostare la minaccia in una cartella isolata (vedi sezione [Quarantena](#)).

Se una minaccia è stata rilevata in un'applicazione installata, non può essere spostata in quarantena. In questo caso l'opzione **In quarantena** non è disponibile.



Ignora per lasciare temporaneamente intatta la modifica nell'area di sistema o la minaccia.



Invia al laboratorio o **Falso positivo** per inviare il file al laboratorio antivirus Doctor Web per l'analisi. L'analisi mostrerà se questa è davvero una minaccia o un falso positivo. Se si è verificato un falso positivo, esso verrà corretto. Per ricevere i risultati dell'analisi, indicare un indirizzo email.

Se il file è stato correttamente inviato al laboratorio, all'oggetto viene automaticamente applicata l'azione **Ignora**.

L'opzione **Invia al laboratorio** è disponibile solo per file eseguibili aggiunti o modificati nell'area di sistema: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.

L'opzione **Falso positivo** è disponibile solo per versioni di minacce e per le minacce nell'area di sistema.



Maggiori informazioni su Internet per aprire la pagina con la descrizione dell'oggetto rilevato sul sito Doctor Web.

6.1.2.1. Minacce nelle applicazioni di sistema

Le applicazioni installate nell'area di sistema in alcuni casi possono eseguire funzioni caratteristiche dei programmi malevoli, per cui Dr.Web può identificare tali applicazioni come minacce.

Per le applicazioni di sistema, così come per qualsiasi applicazione installata, l'opzione **In quarantena** non è disponibile.

Se un'applicazione di sistema può essere rimossa senza compromettere l'operatività del dispositivo o può essere curata, per essa è disponibile l'opzione corrispondente nella versione completa di Dr.Web. Per questo scopo, sul dispositivo devono essere disponibili i permessi di root.

Se un'applicazione di sistema non può essere rimossa senza compromettere l'operatività del dispositivo, l'opzione **Elimina** non è disponibile, ma è possibile utilizzare le seguenti raccomandazioni:

- Arrestare l'applicazione attraverso le impostazioni del dispositivo: nella lista delle applicazioni installate sulla schermata **Impostazioni** > **Applicazioni** selezionare l'applicazione identificata come minaccia, dopodiché sulla schermata con informazioni su di essa premere il pulsante **Interrompi**.



Sarà necessario eseguire questa azione dopo ogni riavvio del dispositivo.

- Disattivare l'applicazione attraverso le impostazioni del dispositivo: nella lista delle applicazioni installate sulla schermata **Impostazioni** > **Applicazioni** selezionare l'applicazione identificata come minaccia, dopodiché sulla schermata con informazioni su di essa premere il pulsante **Disattiva**.
- Se sul dispositivo è installato un firmware custom, è possibile ritornare al software ufficiale del produttore del dispositivo in autonomo o contattando un centro assistenza.
- Se si utilizza il software ufficiale del produttore del dispositivo, provare a contattare l'azienda produttrice per ricevere ulteriori informazioni su questa applicazione.
- Se sul dispositivo sono disponibili i permessi di root, è possibile provare a rimuovere tali applicazioni utilizzando utility specifiche.

Per disattivare l'avviso sulle minacce nelle applicazioni di sistema che non possono essere rimosse senza compromettere l'operatività del dispositivo, spuntare il flag **Applicazioni di sistema** nella sezione **Impostazioni** > **Impostazioni generali**.

6.1.2.2. Modifiche nell'area di sistema

L'area di sistema — area di memoria che viene utilizzata dalle applicazioni di sistema e contiene dati critici per il funzionamento del dispositivo e dati utente sensibili. Se sul dispositivo non sono consentiti i permessi di root, l'area di sistema non è disponibile per l'utente.

Le applicazioni malevole possono ottenere i permessi di root e apportare modifiche all'area di sistema: rimuovere, aggiungere o modificare file o cartelle.

È possibile attivare il controllo dell'area di sistema nelle [impostazioni di Scanner](#). Se il componente rileverà modifiche sospette, avviserà l'utente sulla base dei risultati del [controllo](#).

Modifica	Nome	Tipo
Rimozione di una cartella di file	read-only.area.dir.deleted.threat	Eliminazione dei file di sistema
Rimozione di un file	read-only.area.deleted.threat	Eliminazione dei file di sistema
Aggiunta di una cartella di file	read-only.area.dir.added.threat	File nuovi nell'area di sistema
Aggiunta di un file	read-only.area.added.threat	File nuovi nell'area di sistema
Modifica di un file	read-only.area.changed.threat	Modifica dei file di sistema



Se Scanner rileverà una delle modifiche sopraelencate, i file o le cartelle stessi non necessariamente sono malevoli, ma la modifica può essere stata effettuata da un'applicazione malevola.

Per le modifiche rilevate sono disponibili le seguenti opzioni:

- [Ignora](#).
- [Invia al laboratorio](#) — disponibile solo in caso di aggiunta o modifica di file eseguibili: `.jar`, `.odex`, `.so`, file di formato APK, ELF ecc.
- [Maggiori informazioni su Internet](#).

Il componente informa solo sulle modifiche sopraelencate. Per rilevare un'applicazione malevola che poteva apportare modifiche all'area di sistema, eseguire la [scansione completa](#) del dispositivo.

6.1.3. Applicazioni che bloccano il dispositivo

Dr.Web Light consente di proteggere il dispositivo mobile dai programmi ransomware. I simili programmi sono molto pericolosi. Possono cifrare file conservati nella memoria incorporata del dispositivo o sui supporti rimovibili (come per esempio, una scheda SD). Questi programmi possono bloccare lo schermo e visualizzare su di esso messaggi di riscatto per la decifrazione dei file e lo sblocco del dispositivo.

Le azioni dei programmi ransomware possono colpire le fotografie, i video e documenti dell'utente. Inoltre, questi programmi rubano e trasmettono sui server dei malintenzionati diverse informazioni sul dispositivo infetto (compreso l'identificatore IMEI), informazioni dalla rubrica (nomi dei contatti, numeri di telefono e indirizzi email), monitorano le chiamate in entrata e uscita e sono in grado di bloccarle. Tutte le informazioni raccolte, comprese quelle relative alle chiamate, anche vengono trasmesse sul server di controllo.

I programmi ransomware vengono riconosciuti e rimossi da Dr.Web Light al tentativo di infiltrazione sul dispositivo protetto. Tuttavia, il numero e la diversità di tali programmi sono in continuo aumento. Pertanto, un'applicazione di blocco del dispositivo può essere installato sul dispositivo soprattutto se i database dei virus Dr.Web non venivano aggiornati per qualche tempo e non includono informazioni sui nuovi esemplari.

Se il dispositivo mobile è stato bloccato da un programma ransomware, è possibile sbloccare il dispositivo.

Per sbloccare il dispositivo

1. Entro 5 secondi collegare e scollegare il caricabatterie.
2. Entro i successivi 10 secondi collegare le cuffie.
3. Entro i successivi 5 secondi scollegare le cuffie.
4. Entro i successivi 10 secondi scuotere vigorosamente il dispositivo mobile.



5. Dr.Web Light termina tutti i processi attivi sul dispositivo, compreso il processo avviato dal programma di blocco del dispositivo, dopodiché viene accesa una breve vibrazione (sui dispositivi che hanno questa funzionalità). Quindi si apre la schermata Dr.Web Light.



Notare che con la terminazione dei processi attivi i dati delle altre applicazioni che erano attive al momento del blocco del dispositivo potrebbero andare persi.

6. Dopo lo sblocco del dispositivo, si consiglia di [aggiornare](#) i database dei virus Dr.Web e di eseguire la [scansione rapida](#) del sistema o di rimuovere l'applicazione malevola.


6.2. Database dei virus

Per rilevare le minacce alla sicurezza, Dr.Web Light utilizza database dei virus speciali che contengono informazioni su tutte le minacce informatiche per dispositivi con sistema operativo Android, conosciute dagli specialisti Doctor Web. I database dei virus richiedono un aggiornamento periodico in quanto nuovi programmi malevoli compaiono regolarmente. A tale scopo nell'applicazione è implementata la possibilità di aggiornamento dei database dei virus via internet.


Aggiornamento

I database dei virus vengono aggiornati automaticamente attraverso internet diverse volte al giorno. Se i database dei virus non vengono aggiornati da più di 24 ore (per esempio, in assenza di connessione internet), è necessario avviare l'aggiornamento manualmente.

Per scoprire se è necessario aggiornare manualmente i database dei virus

1. Premere  sulla barra di navigazione.
2. Nella finestra che si è aperta si vedono lo stato dei database dei virus e la data dell'ultimo aggiornamento. Se l'ultimo aggiornamento è stato più di 24 ore fa, è necessario eseguire l'aggiornamento manualmente.

Per avviare l'aggiornamento

1. Premere  sulla barra di navigazione.
2. Nella finestra che si è aperta premere **Aggiorna**.




Subito dopo aver installato l'applicazione, è consigliabile aggiornare i database dei virus in modo che Dr.Web Light possa utilizzare le più recenti informazioni sulle minacce conosciute. Le firme antivirali dei virus, le informazioni sulle loro caratteristiche e sui loro modelli di comportamento vengono aggiornate non appena gli specialisti del laboratorio antivirus Doctor Web rilevano nuove minacce, talvolta fino a diverse volte all'ora.

Impostazioni di aggiornamento

Di default, gli aggiornamenti vengono scaricati automaticamente diverse volte al giorno.

Per consentire o vietare l'uso della rete mobile per il download degli aggiornamenti

1. Premere  sulla barra di navigazione (vedi [Immagine 12](#)).
2. Selezionare la sezione **Database dei virus**.
3. Per non utilizzare la rete mobile per il download degli aggiornamenti, spuntare il flag **Aggiornamento tramite Wi-Fi**.


Se non vengono trovate reti Wi-Fi attive, viene suggerito di utilizzare internet mobile. La modifica di questa impostazione non influisce sull'utilizzo della rete mobile da parte delle altre funzioni dell'applicazione e del dispositivo mobile.



Durante un aggiornamento i dati vengono scaricati attraverso la rete. Per il trasferimento dei dati possono essere applicati costi aggiuntivi. Rivolgersi al proprio operatore di telefonia mobile per i dettagli.

6.3. Statistiche

Dr.Web Light registra le statistiche delle minacce rilevate e delle azioni dell'applicazione.

Per visualizzare le statistiche di funzionamento dell'applicazione, premere l'icona  sulla barra di navigazione e selezionare la voce **Statistiche**.

Visualizzazione delle statistiche

Nella scheda **Statistiche** sono disponibili due sezioni di informazioni (vedi [Immagine 8](#)):

- **Totale.** Contiene informazioni sul numero totale di file controllati e di minacce rilevate e neutralizzate.
- **Eventi.** Contiene informazioni sui risultati delle scansioni tramite Scanner Dr.Web, sullo stato di aggiornamento dei database dei virus, sulle minacce rilevate e le azioni eseguite per neutralizzarle.

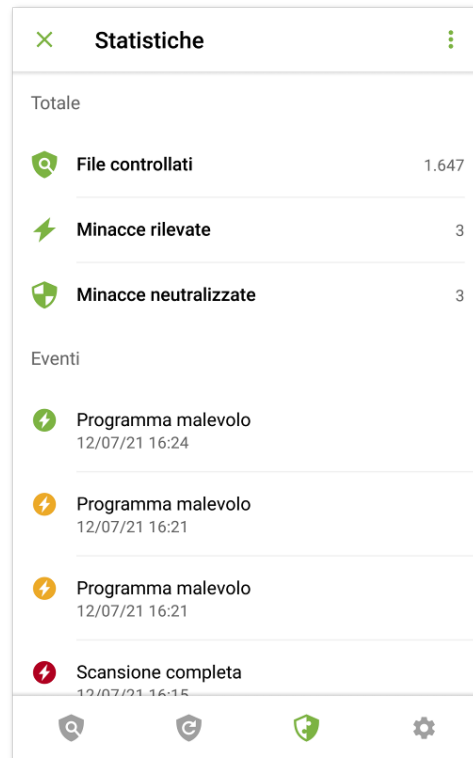




Immagine 8. Statistiche

Pulizia delle statistiche

Per rimuovere tutte le statistiche di funzionamento dell'applicazione raccolte, nella scheda **Statistiche** premere **Menu**  e selezionare la voce **Cancella le statistiche**.

Salvataggio del log degli eventi

È possibile salvare il log degli eventi dell'applicazione per un'analisi in caso di problemi durante l'utilizzo dell'applicazione.

1. Nella scheda **Statistiche** premere **Menu**  e selezionare **Salva i log**.
2. Il log viene salvato nei file `DrWeb_Log.txt` e `DrWeb_Err.txt` situati nella cartella `Android/data/com.drweb/files` nella memoria interna del dispositivo.



Sui dispositivi con Android 11 e versioni successive i log vengono salvati nella cartella `Download/DrWeb`.

6.4. Quarantena

Per le minacce rilevate è disponibile l'opzione di spostamento in quarantena — una cartella specifica progettata per il loro isolamento e l'archiviazione sicura (vedi [Immagine 9](#)).

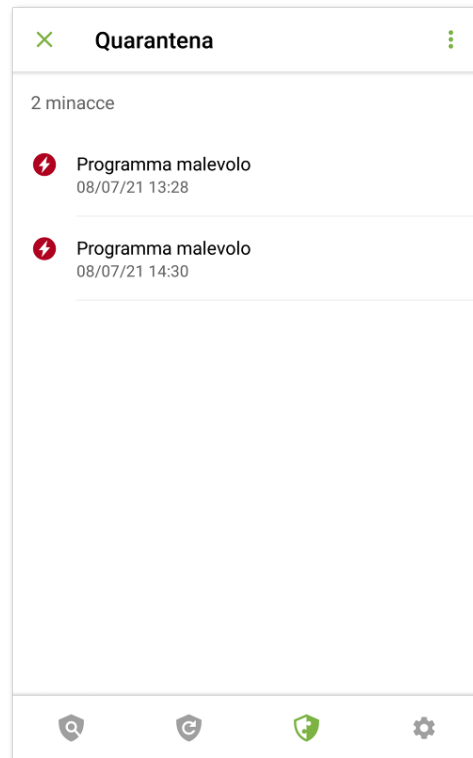



Immagine 9. Quarantena

Visualizzazione della lista degli oggetti in quarantena

Per visualizzare la lista delle minacce spostate in quarantena, premere l'icona  sulla barra di navigazione e selezionare la voce **Quarantena**.

Visualizzazione delle informazioni sulle minacce

Per visualizzare informazioni su una minaccia, premere il suo nome nella lista.

Per ciascuna minaccia è possibile visualizzare le seguenti informazioni:

- nome del file;
- percorso del file;
- data e ora di trasferimento in quarantena.

È possibile espandere la scheda con informazioni su una minaccia facendo scorrere il dito con la scheda verso l'alto. Far scorrere il dito con la scheda verso il basso per comprimerla.

Per visualizzare la lista delle minacce in un archivio contenente più minacce, selezionare l'oggetto corrispondente e premere **Espandi** di fronte alla voce **Minaccia**.



Opzioni disponibili

Per ciascuna minaccia sono disponibili le seguenti opzioni:


- **i** **Maggiori informazioni su Internet** — per visualizzare la descrizione della minaccia sul sito Doctor Web.
- **Ripristina** — per far tornare il file nella cartella in cui si trovava prima dello spostamento in quarantena (utilizzare questa funzione solo se si è sicuri che il file è innocuo).
- **Elimina** — per rimuovere il file da quarantena e dal sistema.
- **Falso positivo** — per inviare il file al laboratorio antivirus Doctor Web per l'analisi. L'analisi mostrerà se il file rappresenta veramente una minaccia o questo è un falso positivo. Se si è verificato un falso positivo, esso verrà corretto. Per ricevere i risultati dell'analisi, indicare il proprio indirizzo email.



L'opzione **Falso positivo** è disponibile solo per varianti di minacce.


Rimozione di tutti gli oggetti da quarantena

Per rimuovere tutti gli oggetti spostati in quarantena:

1. Aprire la sezione **Quarantena**.
2. Sulla schermata **Quarantena** premere **Menu**  e selezionare la voce **Elimina tutto**.
3. Premere **Elimina** per confermare l'azione.
Premere **Annulla** per annullare la rimozione e tornare alla sezione **Quarantena**.

Dimensione quarantena

Per visualizzare informazioni sulla quantità di memoria occupata dalla quarantena e sullo spazio libero nella memoria interna del dispositivo:

1. Aprire la sezione **Quarantena**.
2. Sulla schermata **Quarantena** premere **Menu**  e selezionare la voce **Dimensione**.
3. Premere **OK** per tornare alla sezione **Quarantena**.

6.5. Aiuto all'amico

Il componente **Aiuto all'amico** aiuta a sbloccare il dispositivo di un amico che è bloccato da Antifurto Dr.Web.



Cos'è Antifurto Dr.Web

Antifurto è disponibile nell'applicazione Dr.Web Security Space per Android. Se il dispositivo è stato smarrito o rubato, Antifurto lo blocca. Per sbloccare il dispositivo, è necessario inserire la password. Se il proprietario del dispositivo non ricorda più la password, è possibile aiutarlo a resettare la password e sbloccare il dispositivo.

Come funziona Aiuto all'amico


All'attivazione del componente **Aiuto all'amico** l'utente indica il suo indirizzo email e lo comunica agli utenti di Dr.Web Security Space per Android di cui si fida. Gli utenti di Dr.Web Security Space per Android aggiungono l'utente agli amici in Antifurto. L'utente conferma le richieste di amicizia ricevute.

Se uno degli amici ha bisogno di aiuto per sbloccare il dispositivo, l'amico invierà un avviso all'utente. Dopo aver ricevuto l'avviso, l'utente si mette in contatto con l'amico, scopre il codice di conferma e invia una richiesta di sblocco del dispositivo dell'amico. Dopo aver ricevuto la richiesta di sblocco, Antifurto consente all'amico di resettare la password, dopodiché l'amico può continuare a utilizzare il dispositivo.



Per l'interazione con il dispositivo di un amico, entrambi i dispositivi devono essere connessi a internet. La consegna degli avvisi può richiedere fino a 15 minuti.

Per attivare Aiuto all'amico

1. Sulla barra di navigazione premere l'icona  e selezionare **Aiuto all'amico**.
2. Sulla schermata **Aiuto all'amico** premere **Attiva**.
3. Inserire il proprio indirizzo email e premere **Continua**.



Per aggiungere un amico

1. Comunicare l'indirizzo email impostato all'utente di Dr.Web Security Space per Android affinché possa inviare una richiesta di amicizia.
2. Attendere l'avviso sulla richiesta di amicizia.
3. Premere l'avviso per passare alla schermata **Aiuto all'amico**.
4. Premere la riga con l'indirizzo email dell'amico che ha inviato la richiesta.
5. Premere **Conferma** sulla scheda dell'amico per confermare la richiesta di amicizia.



Se la richiesta di amicizia non è stata accettata o è stata rifiutata dall'utente, l'amico non potrà inviare richieste di sblocco all'utente.

Per modificare il nome di un amico

1. Sulla scheda dell'amico (vedi [Immagine 10](#)) premere .
2. Inserire un nuovo nome dell'amico.
3. Premere  per salvare le modifiche.

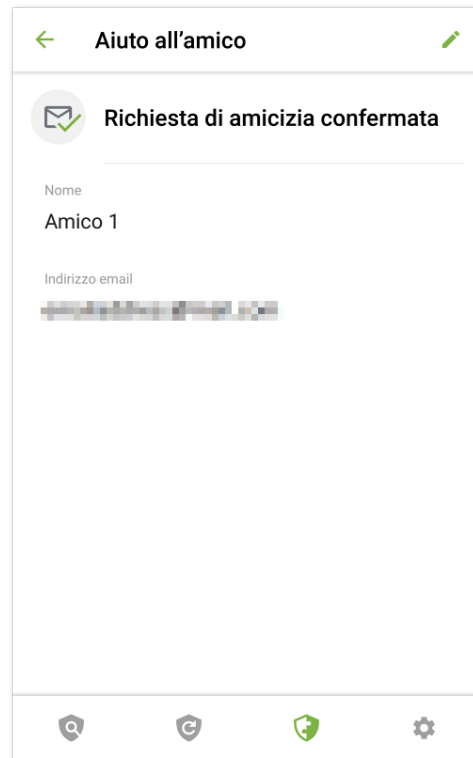


Immagine 10. Scheda dell'amico

È possibile modificare solo il nome dell'amico. Se l'indirizzo email dell'amico è cambiato o non è più utilizzato, è possibile rimuovere l'amico.

Per rimuovere un amico

- Far scorrere il dito con il contatto corrispondente verso sinistra.

Se si rimuove accidentalmente il contatto di un amico di cui non è stata ancora confermata la richiesta di amicizia, è possibile annullare la rimozione premendo **Annulla**.

Per sbloccare il dispositivo di un amico

1. Premere l'avviso di blocco che si è ricevuto dall'amico.
2. Contattare l'amico. Probabilmente il dispositivo è stato smarrito o rubato, e l'avviso è stato inviato da un estraneo.



3. Se l'amico veramente ha bisogno di aiuto per sbloccare il dispositivo, chiedergli il codice di conferma. Il codice di conferma viene visualizzato sulla schermata di blocco sul dispositivo dell'amico.
4. Inserire il codice di conferma e premere **Sblocca** (vedi [Immagine 11](#)).

Se l'avviso di blocco è stato accidentalmente ignorato o chiuso, chiedere all'amico di inviare l'avviso di nuovo.

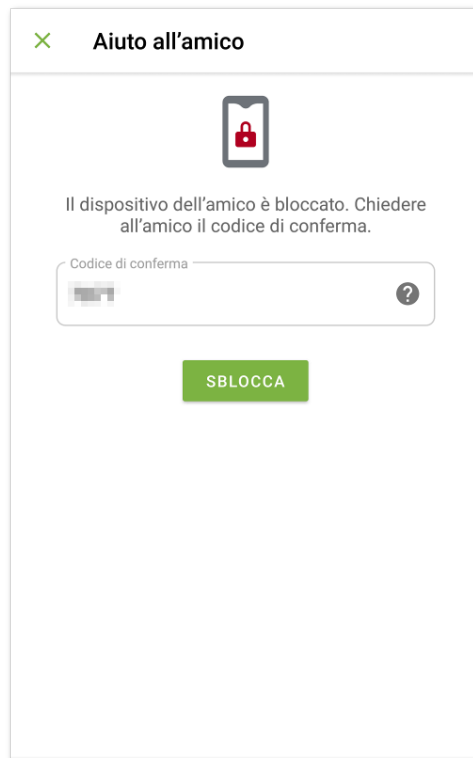




Immagine 11. Codice di conferma dello sblocco

Per disattivare Aiuto all'amico

1. Sulla barra di navigazione premere l'icona  e selezionare **Aiuto all'amico**.
2. Sulla schermata **Aiuto all'amico** premere **Menu**  e selezionare **Disattiva**.



Alla disattivazione di **Aiuto all'amico** tutti gli amici verranno rimossi. Ciascun amico riceverà un avviso che la sua richiesta di amicizia è stata rifiutata.



7. Impostazioni


Per passare alle impostazioni dell'applicazione (vedi [Immagine 12](#)), premere l'icona  sulla barra di navigazione.



Immagine 12. Impostazioni

Sulla schermata **Impostazioni** sono disponibili le seguenti opzioni:

- **Impostazioni generali.** Permette di attivare il tema scuro dell'applicazione, configurare la barra delle notifiche e l'informazione sulle minacce nelle applicazioni di sistema, attivare e disattivare gli avvisi acustici (vedi sezione [Impostazioni generali](#)).
- **Scanner.** Permette di configurare il componente Scanner che esegue una verifica a richiesta dell'utente (vedi sezione [Impostazioni di Scanner Dr.Web](#)).
- **Database dei virus.** Permette di vietare l'uso di internet mobile per l'aggiornamento dei database dei virus (vedi sezione [Database dei virus](#)).
- **Reset delle impostazioni.** Permette di resettare le impostazioni personalizzate e tornare alle impostazioni predefinite (vedi sezione [Reset delle impostazioni](#)).
- **Maggiori informazioni sul sito www.drweb.com.** Permette di passare al sito dell'azienda Doctor Web e visualizzare informazioni sull'applicazione e su altri prodotti dell'azienda.

La schermata **Impostazioni** anche aiuta a ottenere informazioni sul prodotto e sul suo produttore. Nella parte superiore della schermata sotto il nome del prodotto è visualizzata la



versione installata dell'applicazione. Far scorrere il dito con il menu **Impostazioni** verso l'alto per espandere le opzioni di informazione aggiuntive:

- **Guida.** Permette di visualizzare la documentazione dell'applicazione Dr.Web Light.
- **Icone dei social network.** Permette di passare alle pagine dell'azienda Doctor Web su diversi social network.

7.1. Impostazioni generali

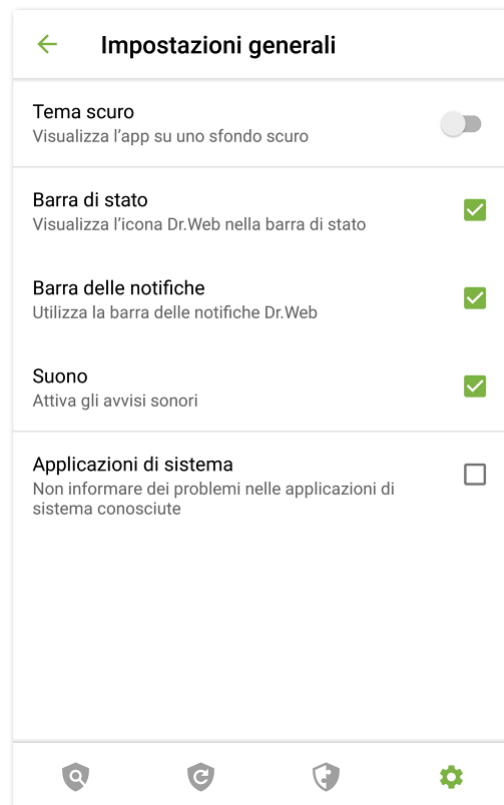


Immagine 13. Impostazioni generali

Sulla schermata **Impostazioni generali** (vedi [Immagine 13](#)) sono disponibili le seguenti opzioni:

- **Tema scuro.** Permette di selezionare lo sfondo scuro o chiaro dell'applicazione.
- **Barra di stato.** Permette di configurare la visualizzazione dell'icona dell'applicazione nella barra di stato. Questa opzione permette inoltre di disattivare la visualizzazione del pannello Dr.Web nell'area delle notifiche (vedi sezione [Barra delle notifiche](#)).



L'impostazione non è disponibile sui dispositivi con Android 8.0 o versioni successive.



- **Barra delle notifiche.** Permette di determinare l'aspetto del pannello Dr.Web nell'area delle notifiche. Se l'opzione è attivata, viene utilizzato il pannello Dr.Web. Se l'opzione è disattivata, il pannello ha l'aspetto di un pannello di notifica Android standard.
- **Suono.** Permette di configurare gli avvisi sonori per segnalare che una minaccia è stata rilevata, rimossa o messa in quarantena. Di default gli avvisi sonori sono attivati.
- **Applicazioni di sistema.** Permette di attivare o disattivare l'avviso sulle [minacce nelle applicazioni di sistema](#) che non possono essere rimosse senza compromettere l'operatività del dispositivo. Di default questa opzione è disattivata.

7.2. Reset delle impostazioni

È possibile resettare le impostazioni personalizzate dell'applicazione e ripristinare le impostazioni di default in qualsiasi momento.

Per resettare le impostazioni

1. Sulla schermata delle impostazioni (vedi [Immagine 12](#)) nella sezione **Reset delle impostazioni** selezionare la voce **Reset delle impostazioni**.
2. Confermare di voler ritornare alle impostazioni predefinite.



Indice analitico

A

- aggiornamento
 - database dei virus 26
 - Dr.Web 9
- Aiuto all'amico 30
- applicazioni di blocco del dispositivo 25
- applicazioni di sistema 23
- area di sistema 24
- avvisi 13

B

- barra delle notifiche 14
 - impostazioni 35
- barra di navigazione 11
- barra di stato 11, 12

C

- componenti 17
 - Scanner Dr.Web 17
- Contratto di licenza 10

D

- database dei virus
 - aggiornamento 26
 - aggiornamento manuale 26
 - impostazioni di aggiornamento 27

F

- falso positivo 19, 23
- funzioni 6

I

- impostazioni 34
 - aggiornamento dei database dei virus 27
 - barra delle notifiche 35
 - impostazioni generali 35
 - invio delle statistiche 35
 - reset 34, 36
- iniziare a utilizzare 10
- installazione
 - da Google Play 8
- installazione da Google Play 8
- interfaccia 11
 - barra di navigazione 11
 - barra di stato 11, 12

- schermata principale 11
- widget 15

- invio delle statistiche 10, 35
- invio di un file al laboratorio 19, 23

L

- laboratorio antivirus 19
- log
 - degli eventi 28

M

- minacce 20
 - applicazioni di blocco del dispositivo 25
 - applicazioni di sistema 23
 - area di sistema 24
 - elimina 22
 - falso positivo 23
 - ignora 23
 - invia al laboratorio 23
 - maggiori informazioni su Internet 23
 - programmi ransomware 25
 - quarantena 28
 - rimuovere tutto 22
 - sposta in quarantena 23
 - tutto in quarantena 22

N

- neutralizzazione delle minacce 20
- neutralizzazione delle minacce una per una 22
- neutralizzazione di più minacce 22

O

- Origins Tracing 5

P

- per iniziare 10
- permessi 10
- programmi ransomware 25
- protezione antivirus 17
 - applicazioni di blocco del dispositivo 25
 - applicazioni di sistema 23
 - area di sistema 24
 - neutralizzazione delle minacce una per una 22
 - neutralizzazione di più minacce 22
 - programmi ransomware 25
 - risultati del controllo 20



Indice analitico

protezione antivirus 17
Scanner Dr.Web 17

Q

quarantena 28
dimensione 30

R

requisiti di sistema 7
reset delle impostazioni 34, 36
rilevamento di minacce 20
applicazioni di sistema 23
area di sistema 24
rimozione di Dr.Web 9
risultati del controllo 20

S

Scanner Dr.Web 17
impostazioni 20
scansione completa 18
scansione personalizzata 18
scansione rapida 18
statistiche 20
scansione
completa 18
falso positivo 19
personalizzata 18
rapida 18
scansione completa 18
scansione personalizzata 18
scansione rapida 18
schermata principale 11
statistiche 27
pulizia 28
salvataggio del log 28
Scanner Dr.Web 20
visualizzazione 27
stato di protezione 12
suono 35

V

versione completa dell'applicazione 11

W

widget 15

