

Protezione e velocità del sito

Come funziona il sistema che protegge e velocizza il tuo sito, cosa fare se compare la pagina "Attack blocked", la cache delle pagine e il certificato HTTPS.

- [Come funziona la protezione del tuo sito](#)
- [Ho visto la pagina "Attack blocked"](#)
- [Ho modificato il sito ma non vedo le modifiche](#)
- [Il lucchetto \(HTTPS\) e il certificato di sicurezza](#)
- [Domande frequenti](#)

Come funziona la protezione del tuo sito

Quando qualcuno apre il tuo sito, la sua richiesta non arriva direttamente al server dove il sito è installato. Passa prima da un **sistema di protezione** che WhiteReady mette davanti a tutti i siti che ospita.

Puoi immaginarlo come la **reception di un palazzo**: chi entra passa dal bancone, la reception controlla che sia tutto in regola e lo accompagna all'ufficio giusto. Chi si comporta in modo sospetto viene fermato prima di arrivare alle scale.



Questo sistema fa quattro cose per te, senza che tu debba configurare nulla:

Cosa fa	Cosa significa per te
Blocca gli attacchi	Controlla ogni richiesta e ferma i tentativi di intrusione più comuni: programmi automatici che cercano password, falle nei plugin, file riservati.
Gestisce il certificato di sicurezza (HTTPS)	Il lucchetto nella barra del browser. Lo attiviamo e lo rinnoviamo noi, prima che scada.
Rende il sito più veloce	Per molti siti WordPress tiene pronta una copia delle pagine e la consegna subito, senza far lavorare ogni volta il server.
Tiene lontano il traffico inutile	Robot aggressivi e scansioni automatiche non consumano le risorse del tuo sito.

Nella grande maggioranza dei casi **non ti accorgerai mai della sua presenza**. Le pagine che seguono spiegano i pochi casi in cui potresti notarlo e cosa fare.

Ho visto la pagina "Attack blocked"

A volte, invece della pagina che ti aspettavi, compare una schermata con un testo simile a questo:

Attack blocked by web application protection Check Point's Application Security has detected an attack and blocked it. Incident Id: 649fd1bf-39a4-4e36-ab63-eac805ed952b



Attack blocked by web application protection

Check Point's **Application Security** has detected an attack and blocked it.

Incident Id: c7ce0648-7a77-4fe5-9a28-c0ddc713d4f6

← copia questo codice

Vuol dire che il sistema di protezione ha giudicato sospetta la richiesta che stavi facendo e l'ha fermata. **Il sito non è stato danneggiato e nessun dato è andato perso**: semplicemente quell'operazione non è stata eseguita.

Perché può succedere anche a te

Il sistema riconosce gli attacchi da come sono fatte le richieste. Ogni tanto un'operazione del tutto normale "assomiglia" a un attacco. Succede soprattutto quando:

- **carichi un plugin o un tema** in formato ZIP dalla bacheca di WordPress;
- **salvi un testo che contiene codice**: script, codici di tracciamento, HTML copiato da altri siti;
- **compili un modulo** con parole o simboli insoliti;

- **usi una password** con molti caratteri speciali.

Sono i cosiddetti **falsi positivi**: il sistema ha preferito essere prudente.

Cosa fare

1. **Non riprovare più volte di seguito.** Molti tentativi ravvicinati possono far aumentare la sorveglianza sul tuo indirizzo.
2. **Copia il codice "Incident Id":** è la riga lunga con lettere e numeri. Se non riesci a copiarlo, fai uno screenshot della pagina.
3. **Apri un ticket** scrivendo a supporto@whiteready.com (oppure dal portale ticket.whiteready.com) e indica:
 - il codice Incident Id;
 - il sito su cui stavi lavorando;
 - l'ora, anche approssimativa;
 - cosa stavi facendo (per esempio "stavo caricando il plugin X", "stavo salvando la pagina Contatti").

Con il codice ritroviamo la richiesta esatta, capiamo cosa ha fatto scattare il blocco e, se è un falso positivo, correggiamo la regola. Per i plugin e i temi possiamo anche installarli noi direttamente sul server.

Per aprire un ticket: scrivi a supporto@whiteready.com oppure usa il portale

ticket.whiteready.com

Telefono: +39 011 6602616

E se a vedere la pagina è un tuo visitatore?

Se un tuo cliente ti segnala la stessa pagina mentre compila un modulo del tuo sito, fatti mandare il codice Incident Id e l'ora, e inoltraci tutto aprendo un ticket a supporto@whiteready.com. Vale la stessa procedura.

Ho modificato il sito ma non vedo le modifiche

Per rendere i siti più veloci, il sistema di protezione può tenere una **copia pronta delle pagine** (la cosiddetta *cache*) e consegnarla subito ai visitatori.

Sui siti WordPress con la cache attiva

- **Quando pubblichi o modifichi** un articolo, una pagina o un prodotto, il sito avvisa automaticamente il sistema, che aggiorna la copia della pagina, della home e delle pagine collegate (categorie, archivi). Di norma le modifiche sono visibili **entro pochi secondi**.
- **Mentre sei collegato all'area di amministrazione**, vedi sempre la versione aggiornata del sito: la cache vale solo per i visitatori.
- Il carrello, il checkout, l'area clienti e le pagine di accesso **non vengono mai messi in cache**.

Se dopo un minuto la modifica non si vede ancora

1. **Aggiorna la pagina forzando il browser** a ricaricarla: `Ctrl + F5` su Windows, `Cmd + Maiusc + R` su Mac.
2. **Prova da una finestra in incognito** o da un altro dispositivo: a volte è il tuo browser che conserva la vecchia versione.
3. Se la modifica non riguarda un contenuto ma la grafica o i file del sito (tema, fogli di stile, immagini sostituite con lo stesso nome), può servire qualche ora: in quel caso **apri un ticket** a supporto@whiteready.com e svuotiamo noi la copia.

Contenuti che cambiano da soli

Se il tuo sito mostra dati che cambiano senza passare dall'editor, per esempio prezzi o disponibilità importati da un gestionale, listini aggiornati da un altro programma o feed esterni, **diccelo** aprendo un ticket a supporto@whiteready.com. Possiamo ridurre la durata della copia o escludere quelle pagine.

Il lucchetto (HTTPS) e il certificato di sicurezza

Il **certificato di sicurezza** è quello che fa comparire il lucchetto nella barra degli indirizzi e permette di usare `https: //`. Protegge i dati che i visitatori inviano al sito, per esempio password, moduli e ordini.

Cosa facciamo noi

- **Attiviamo il certificato** quando il sito viene messo online.
- **Lo rinnoviamo automaticamente** prima della scadenza: non devi ricordarti niente.
- **Portiamo i visitatori sempre su HTTPS**, anche se scrivono l'indirizzo senza `https: //`.

Dal 2026 i certificati durano meno, fino a un massimo di 199 giorni: trovi i dettagli nell'annuncio [Validità del certificato SSL ridotta a 199 giorni](#). Per i certificati che gestiamo noi non cambia nulla: il rinnovo è automatico.

Cosa devi sapere tu

- **Se gestisci tu i DNS del dominio** (presso un altro fornitore), il dominio deve continuare a puntare ai nostri indirizzi. Se lo sposti, il certificato non si potrà più rinnovare e il sito risulterà "non sicuro". Prima di modificare i DNS, **chiedici gli indirizzi corretti** aprendo un ticket a supporto@whiteready.com.
- **Se aggiungi un nuovo indirizzo** al sito (per esempio `shop.tuodominio.it`), oppure la versione con o senza `www`), avvisaci con un ticket a supporto@whiteready.com: va aggiunto anche al certificato.
- **Se vuoi un certificato commerciale** (per esempio con validazione dell'azienda), apri un ticket a supporto@whiteready.com prima di acquistarlo: ti diciamo come procedere.

"La connessione non è privata": cosa fare

Se il browser mostra un avviso di sicurezza sul tuo sito:

Così appare l'avviso in Chrome (in italiano il titolo è «La connessione non è privata»):



Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). [Learn more about this warning](#)

NET::ERR_CERT_DATE_INVALID

Advanced

Back to safety

1. controlla che l'indirizzo sia scritto correttamente;
2. controlla la data e l'ora del tuo computer (se sono sbagliate, tutti i certificati sembrano scaduti);
3. se l'avviso resta, **apri un ticket** a supporto@whiteready.com indicando l'indirizzo esatto della pagina.

Domande frequenti

Il sistema di protezione rallenta il mio sito? No. Il controllo richiede una frazione di secondo e, con la cache attiva, le pagine arrivano anzi più velocemente di prima.

Nelle statistiche del sito (Google Analytics, Matomo, log) vedo gli indirizzi reali dei visitatori? Sì. Il sistema passa al tuo sito l'indirizzo reale di chi lo visita.

Ho un plugin di sicurezza su WordPress (Wordfence e simili). Devo toglierlo? No, puoi tenerlo: le due protezioni si sommano. Se però il plugin blocca degli indirizzi "a caso" o blocca il sito intero, apri un ticket a supporto@whiteready.com prima di modificarne le impostazioni.

Ho un plugin di cache su WordPress. Va bene? Sì. Se noti comportamenti strani (pagine vecchie che restano, carrello che non si aggiorna), segnalacelo con un ticket a supporto@whiteready.com: verifichiamo che le due cache non si ostacolino.

Perché non riesco ad aprire file come `.env`, `.sql`, `.log` o `.bak` del mio sito? Sono file che spesso contengono password o copie del database, e sono tra i primi che cercano gli attacchi automatici. Il sistema li blocca **sempre** con un errore 403, su tutti i siti. Se ti serve scaricarne uno, usa l'FTP o apri un ticket a supporto@whiteready.com.

Lo sviluppatore del mio sito deve configurare qualcosa? No. Deve solo sapere che il sito è protetto da un firewall applicativo: se durante il lavoro vede la pagina "Attack blocked", segue le istruzioni della pagina [Ho visto la pagina "Attack blocked"](#) e apre un ticket a supporto@whiteready.com.

Posso disattivare la protezione? Non è consigliabile e non è possibile farlo da soli. Se un'operazione legittima viene bloccata, la soluzione è correggere la regola che la ferma, e lo facciamo noi.