



La rivoluzione nella sicurezza.  
Performance estreme.  
Gestione minimale.

L'innovativa tecnologia Webroot combinata alla potenza del Cloud da vita a Webroot SecureAnywhere – Endpoint Protection per bloccare le minacce note e neutralizzare gli attacchi zero-day sconosciuti.

## Webroot

### IN EVIDENZA

#### La miglior protezione contro il malware conosciuto e sconosciuto

- Tecnologia rivoluzionaria di riconoscimento del comportamento e dei file pattern.
- Capisce se l'attività di un PC è legittima o pericolosa.
- Elimina di fatto la finestra di vulnerabilità delle nuove minacce.

#### Estremamente veloce e semplice da installare

- Il client/agent per la sicurezza degli endpoint più piccolo del mondo (<1MB).
- L'installazione richiede tipicamente meno di 6 secondi\*.
- Coesiste con altre applicazioni software o soluzioni per la sicurezza.

#### Non rallenta i PC né ostacola la produttività utente

- La scansione iniziale richiede meno di due minuti, quelle successive, meno di un minuto\*.
- Utilizzo minimale della CPU durante le scansioni.
- Sofistiche tecniche di remediation eliminano il reimaging dei sistemi.

#### Sempre aggiornati, sempre protetti

- Niente più pesanti file di aggiornamento quotidiano che consumano banda.
- Tutti gli utenti sono istantaneamente protetti contro qualsiasi nuova minaccia.

#### Note:

\*PassMark Software, "Webroot SecureAnywhere vs. Traditional Anti-virus".

## Webroot SecureAnywhere Endpoint Protection

Webroot SecureAnywhere – Endpoint Protection offre un approccio rivoluzionario alla protezione degli endpoint contro il malware. La soluzione **combina l'innovativa tecnologia Webroot per il riconoscimento del comportamento e dei file pattern con la potenza del cloud computing** per bloccare le minacce note e neutralizzare gli attacchi zero-day sconosciuti con più efficacia rispetto a chiunque altro.

Grazie al client di sicurezza per endpoint più leggero e veloce del mondo, le **scansioni risultano incredibilmente rapide** - di norma meno di due minuti\* - senza rallentare il lavoro degli utenti. E dal momento che la tecnologia è veramente real-time, la sicurezza risulta sempre aggiornata garantendo protezione contro tutte le minacce e gli attacchi più recenti **senza il fastidio di dover gestire gli aggiornamenti ai file delle signature**, o "firme", tradizionalmente impiegati per intercettare il malware.

### CARATTERISTICHE

#### Potenti funzioni di rilevamento malware.

Implementa la più avanzata protezione in tempo reale degli endpoint contro malware noto e ignoto eliminando di fatto la finestra di vulnerabilità che intercorre tra l'emergere di una minaccia e il suo rilevamento.

#### Protezione offline.

Blocca gli attacchi quando un endpoint è scollegato dalla rete con apposite policy di esecuzione dei file applicabili ai dischi locali, ai drive USB, ai CD e ai DVD.

#### Potenti funzionalità euristiche.

I parametri euristici possono essere regolati in base alla tolleranza ai rischi per l'esecuzione dei file. I parametri euristici comprendono:

**Advanced** analizza i nuovi programmi cercando azioni sospette tipiche del malware.

**Age** analizza i nuovi programmi in base a quanto tempo un file simile è presente all'interno della community Webroot.

**Popularity** analizza i nuovi programmi in base alla frequenza di utilizzo o modifica di un file all'interno della community Webroot.

#### Neutralizzazione malware.

Un engine completo per il rilevamento e la rimozione identifica le minacce note e ignote compresi rootkit e altri software pericolosi eliminandone i file dai sistemi degli utenti.

#### Webroot Intelligence Network.

Rilevamento e analisi delle minacce in tempo reale attraverso il più grande database cloud di oggetti estraibili del mondo composto da oltre 250 milioni di file e relative caratteristiche comportamentali.

#### Deployment istantaneo.

Il deployment avviene tramite un file di installazione MSI pacchettizzato, con un tool per deployment personalizzati, o con un link tramite cui scaricare l'eseguibile.

**Facile da gestire**

- Gestione centralizzata di tutti gli endpoint.
- Gestione e reporting automatizzati.
- Nessuna gestione on-premise management di hardware o software server.

**Protezione online e offline**

Controlli di policy utente separati per la gestione dell'uso degli endpoint scollegati dalla rete.

**Webroot sviluppa soluzioni di sicurezza informatica in ambito Cloud e le distribuisce a livello mondiale, sia per utenti privati che per aziende.**

**Webroot SecureAnywhere è l'innovativo software per la sicurezza degli endpoint basato su Cloud.**

<http://www.achab.it/Webroot>

**Compatibilità software.**

Compatibile con altre applicazioni software comprese altre soluzioni per la sicurezza degli endpoint, così da semplificare il deployment a fianco delle applicazioni già esistenti.

**Firewall applicativo / monitoraggio di sistema.**

Un sofisticato firewall basato su cloud protegge gli utenti quando si trovano al di fuori del gateway aziendale rafforzando il firewall di Microsoft Windows per offrire il pieno controllo delle connessioni in entrata e in uscita senza appesantire inutilmente le risorse degli endpoint. Gestendo e monitorando tutto il traffico in uscita, il firewall protegge dagli attacchi e assicura che solo le applicazioni approvate per policy possano comunicare con la rete. Riconosce inoltre automaticamente i programmi di cui sia nota la tipologia (leciti o pericolosi) in modo da evitare di infastidire gli utenti con pop-up continui o costringerli a prendere decisioni non informate.

**Supporto di server e server virtuali.**

Oltre a supportare i PC Windows fisici, Webroot Secure Anywhere può supportare anche gli ambienti server e i server virtuali Windows.

**Architettura cloud distribuita ridondante.**

Un'architettura composta da più datacenter globali che supportano le sedi locali e gli utenti mobili attraverso il datacenter più vicino con eccellenti livelli di ridondanza.

**VANTAGGI****Sicurezza rivoluzionaria**

La rivoluzionaria sicurezza cloud di Webroot elimina nella pratica le finestre di vulnerabilità che esistono con altre soluzioni per endpoint garantendo una vera protezione in tempo reale contro tutte le tipologie di minacce.

- Elimina di fatto l'intervallo di esposizione al rischio che intercorre tra il rilascio di un exploit e la sua intercettazione e neutralizzazione.
- Una particolare tecnologia per il riconoscimento di comportamenti e file pattern capisce se l'attività di un PC è legittima o pericolosa.
- Controllo quasi istantaneo dei file su Webroot Intelligence Network, un database cloud contenente centinaia di milioni di file e comportamenti per capire le vere intenzioni di un codice eseguibile.
- Una intelligenza avanzata discrimina le minacce conosciute da quelle mai osservate prima proteggendo i PC da tutte le minacce note, nuove e zero-day.
- La protezione offline tutela gli endpoint non connessi a Internet con potenti funzioni euristiche e la capacità di bloccare porte e dispositivi come drive USB, CD e DVD.
- Webroot Intelligence Network raccoglie costantemente informazioni su nuovi file potenzialmente pericolosi da Internet e dai clienti Webroot mettendole istantaneamente in condivisione per garantire una protezione aggiornata.

**Performance di alto livello**

Webroot SecureAnywhere – Endpoint Protection definisce nuovi standard in termini di deployment, velocità di scansione, consumo delle risorse di sistema e dimensioni sull'endpoint in modo da far risparmiare tempo e denaro.

- Client ultra-leggero: il più piccolo del mondo, meno di 1MB di dimensioni;
- Si scarica e si installa in 6 secondi.
- Funziona con un consumo di CPU minimo per evitare di rallentare gli utenti finali.
- Richiede pochissimo spazio su disco; non occorre un database locale delle minacce.
- Scansioni velocissime impiegano meno di due minuti\* rispetto alle intere ore di molte altre soluzioni per la sicurezza.
- Prestazioni migliorate su PC con minimi requisiti di sistema.
- È in grado di coesistere con altri prodotti per la sicurezza eliminando la necessità di disinstallare altre soluzioni prima della migrazione.
- Massimizza sicurezza e produttività funzionando in maniera discreta.

\*Dopo la scansione iniziale del PC, le scansioni complete del sistema richiedono normalmente due minuti o meno.