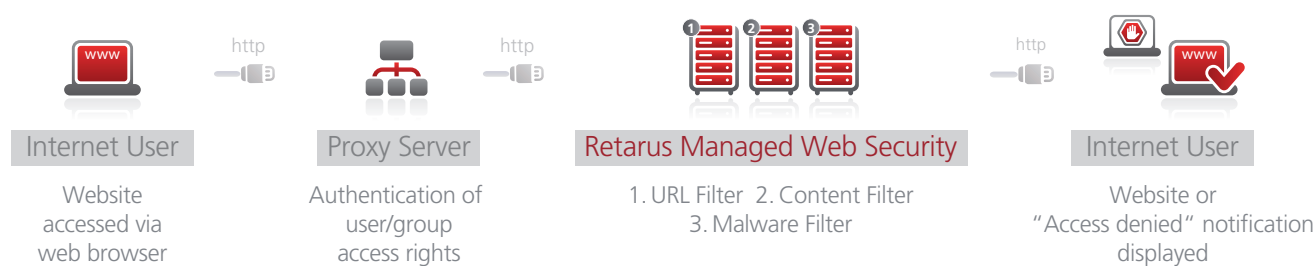


I siti web infetti da virus e spyware, l'uso eccessivo della rete da parte dei vostri dipendenti e i contenuti indesiderati mettono a rischio la sicurezza dell'infrastruttura informatica della vostra impresa e pregiudicano la produttività. Per garantire l'ottemperanza delle norme di utilizzo di internet nelle imprese, gli analisti IT di Gartner consigliano caldamente di impiegare un filtro web. Il servizio Retarus Managed Web Security offre un'ampia protezione da minacce e da contenuti indesiderati della rete. In tal modo fate valere le vostre norme di utilizzo e migliorate durevolmente la sicurezza della vostra impresa. Un reporting dettagliato vi assicura anche una completa trasparenza dell'utilizzo di internet da parte dei vostri dipendenti.

### Funziona così



### I vostri vantaggi

Efficace protezione da spyware, virus e contenuti web indesiderati

Rispetto delle disposizioni sull'utilizzo del web

Comoda configurazione tramite categorie e liste

Reporting trasparenti per dominio, sito web e categorie di filtraggio

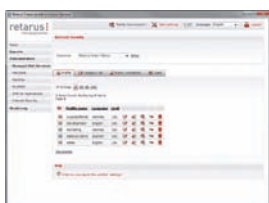
Sincronizzazione con la vostra rubrica



Protezione affidabile da contenuti indesiderati



Comoda configurazione tramite categorie



Controllo dell'utilizzo della rete in base a profili

## Filtraggio efficace – navigazione sicura

Possibilità di filtraggio URL, riconoscimento automatico di malware, funzioni di reporting: secondo Gartner sono queste le richieste principali poste ad una soluzione di filtraggio web. Con il servizio Retarus Managed Web Security controllate in modo efficace l'utilizzo di internet da parte dei vostri dipendenti all'interno della vostra impresa: per mezzo di più di 80 categorie di filtraggio potete bloccare contenuti web indesiderati come ad esempio chat, social network, giochi ed erotismo. La produttività del vostro personale non ne risente e soddisfatte inoltre anche le disposizioni di legge se ad esempio lavorano presso di voi apprendisti minorenni per i quali dovette bloccare contenuti pericolosi. I filtri vengono aggiornati da noi continuamente per garantire sempre una protezione adeguata e sicura.

## Controllo attraverso una configurazione flessibile

Potete controllare gli accessi al web in modo ancora più preciso per mezzo di cosiddette liste black & white con le quali - a seconda dell'utente o del gruppo di utenti - bloccate o consentite l'accesso a determinati siti. Potete ad esempio impedire l'utilizzo di alcuni social network come Facebook e permettere invece l'uso di altri come Xing. In ogni momento fate valere comunque le vostre norme di utilizzo di internet. I siti web che non sono contenuti in blacklist o altre liste di filtraggio si possono facilmente bloccare in base a delle liste di parole categorizzate. In questo caso, qualora una parola dovesse oltrepassare il valore limite da voi predefinito, la pagina web viene immediatamente bloccata. Su richiesta adattiamo le liste alle vostre esigenze – per il massimo controllo dei contenuti web.

## Sicurezza per la vostra infrastruttura

Il servizio Retarus Managed Web Security protegge in modo ottimale la vostra infrastruttura da siti web contenenti virus o spyware. L'infrastruttura di Retarus riconosce la presenza di programmi maligni già nel momento in cui si cerca di accedere a un tale sito e impedisce il caricamento delle relative pagine. Inoltre potete anche impedire il download HTTP di singoli tipi di file come ad esempio file .EXE, .LNK o .SCR. In questo modo evitate che programmi maligni raggiungano i terminali dei posti di lavoro.

## Trasparenza grazie a reporting dettagliati

La Gartner consiglia di affidarsi a una soluzione che permetta un'autenticazione delle utenze così come la facile gestione dei diritti di accesso. Un servizio, dunque, che offre la possibilità di confrontare i dati con rubriche esistenti. Sul nostro portale web di amministrazione potete configurare comodamente le categorie e le liste e creare le utenze, i gruppi di utenti e i profili. L'autenticazione degli utenti avviene tramite un proxy dell'impresa. I profili si possono sincronizzare con la vostra active directory o con altri sistemi di elenchi. I reporting dettagliati rendono trasparente l'uso della rete da parte dei vostri dipendenti. Potete così venire a sapere quando e con che frequenza sono stati richiamati singoli siti web o domain nel corso di un determinato arco di tempo e riconoscerne la relativa categoria di filtraggio. A proposito: la protezione può essere estesa anche ai dipendenti in servizio esterno. Fate voi stessi una prova!