

# Ferma i virus prima che entrino nella rete



## SICUREZZA PROATTIVA

Protegge la tua rete in modo preventivo, bloccando virus e malware prima che entrino in rete.

Al giorno d'oggi **gran parte delle minacce informatiche parte da un click** sul link sbagliato o dalla visita su un sito malevolo e, purtroppo, gli utenti difficilmente sono in grado di distinguere un link legittimo da uno contenente un virus.

**Spesso a pagarne le conseguenze sono aziende come la tua**, che si ritrovano a subire furti di dati e denaro o ad avere i sistemi IT completamente bloccati da un ransomware.

Quello che ti serve è **una soluzione di sicurezza che blocca le minacce prima che entrino nelle reti** e protegge gli utenti anche quando sono fuori sede.

**Una soluzione economica e proattiva** che costituisce una barriera affidabile contro malware spyware e virus e di impedire l'accesso a determinati siti.

## > I VANTAGGI

- » **Aumenti la sicurezza** perché virus e malware vengono fermati prima che entrino nei loro sistemi.
- » Garantisci **protezione completa e sempre attiva alla tua azienda**, grazie alle policy applicate anche al di fuori della rete aziendale.
- » **Riduci il rischio cryptovirus**, perché riesci a bloccare i link contenuti nelle email e un eventuale virus non riuscirà a contattare il suo server di riferimento.
- » Hai maggiore **controllo sull'utilizzo di Internet** nella tua azienda, filtrando l'accesso a particolari siti, con regole personalizzabili.

## > COME FUNZIONA

### TECNOLOGIE ALL'AVANGUARDIA, SICUREZZA MULTILIVELLO

Una soluzione di sicurezza di questo tipo utilizza un sistema di **sicurezza multilivello** real-time che blocca le minacce prima che entrino nelle reti, infatti esegue un **controllo immediato** di tutti gli indirizzi web digitati o cliccati, bloccando eventuali malware prima che l'utente possa accedere al sito o bloccando l'accesso al sito stesso.

Si avvale di **tecnologie all'avanguardia**, tra le quali una funzionalità anti-phishing dinamica per evitare gli attacchi di phishing zero-hour; **identifica istantaneamente malware e spam**, rilevando in questo modo le minacce zero-day senza bisogno di firme o aggiornamenti.

Questa soluzione identifica gli indirizzi IP associati ad attività pericolose. Oltre a offrire un metodo efficace per prevenire le minacce web sconosciute, offre agli amministratori **visibilità sul traffico di rete pericoloso**.

Gli utenti che cliccano sui link contenuti nelle email e poi si infettano con un cryptovirus saranno un ricordo del passato!

### PROTEZIONE DEGLI UTENTI IN ROAMING

Oltre a proteggere le reti bloccando virus e malware prima che infettino i sistemi, questa soluzione **protegge anche gli utenti mobili** che si spostano con il proprio notebook. Puoi infatti impostare delle policy di sicurezza e filtraggio della navigazione che proteggono gli utenti anche quando escono dal perimetro di rete aziendale e si collegano in hotel, in aeroporto o in altri luoghi dove non c'è modo di controllare la sicurezza della connessione.