

> ANTIVIRUS

Norman Virus Control 5.80

SOFTWARE
INCLUSO NEL CD 1

Un antivirus venuto dal freddo ma con una marcia in più

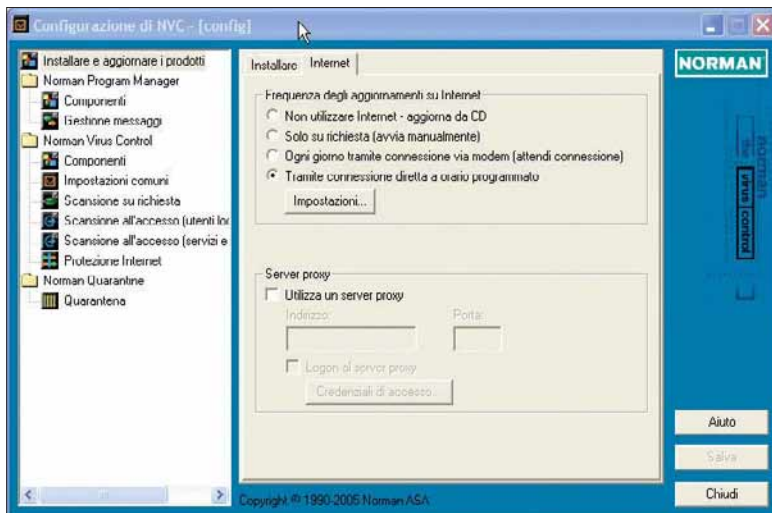
Norman, software house scandinava, da qualche anno sviluppa pacchetti e prodotti di pregio articolati in base alle esigenze di protezione e gestione del cliente. Norman Virus Control è sicuramente il perno su cui appoggia tutta la tecnologia successivamente diversificata, dimostrandosi, all'atto dell'utilizzo, un prodotto tra i migliori presenti sul mercato.

Sebbene non possa essere considerato un pacchetto di Internet Security nel senso più ampio del termine (d'altro canto Norman distribuisce un prodotto di questo tipo, di fascia superiore, ad un prezzo leggermente più alto), Norman Virus Control è molto di più di un semplice antivirus. In quest'ultimo ambito si tratta sicuramente di un prodotto allineato con le ultime tecnologie, basato com'è sulla combinazione di un motore euristico e di un sistema a scansione agganciato a una libreria particolarmente ricca (oltre 100.000 firme virali) aggiornata regolarmente a ritmo giornaliero e, nei casi di maggior virulenza, anche più volte al giorno.

Accanto a questa forma di difesa, peraltro simile a quella di quasi tutti gli altri pacchetti presenti sul mercato, se ne affianca una, peraltro non originale ma qui sapientemente implementata, definita SandBox; si tratta di una forma preventiva di gestione dei file sospetti che vengono analizzati all'interno di un ambiente isolato e sicuro per verificare il loro effettivo comportamento.

Il principio si basa sul fatto che file sconosciuti o sospetti, non ancora riconoscibili dall'antivirus, potrebbero penetrare nel nostro ambiente di lavoro causando danni. Il SandBox è un'area blindata in cui file a rischio vengono spostati per controllarne le azioni ed eseguire una valutazione del loro modo di agire.

In altri termini Norman



crea, all'interno del nostro sistema, un computer virtuale isolato dall'ambiente reale e gestito completamente dal motore di scansione antivirus proprietario, che genera un ambiente completo di Bios, hardware, dischi rigidi, memoria Ram, tutto completamente simulato. In esso il sistema emula tutte le fa-

si di funzionamento di un normale Pc, fin dalla sequenza di avvio, seguita dal caricamento del file e del sistema operativo e dalla shell dei comandi dell'unità simulata. Questo ambiente contiene tutte le directory e i file di sistema, nient'altro che un ambiente teorico del tutto identico al sistema dei dischi rigidi fisici.

Il file sospetto viene così inserito nel disco rigido simulato e lasciato libero di eseguire le sue operazioni. Il probabile file infetto non riscontra alcuna differenza tra

▲ **L'interfaccia principale** Potente, efficace e dotata di funzioni complementari e interessanti, Norman si è dimostrato particolarmente disponibile agli aggiornamenti, non solo delle librerie ma anche del codice.

questo ambiente e quello reale ed è libero di svolgere qualsiasi operazione, come infettare ed eliminare file, replicarsi in rete, connettersi a un server Irc, inviare posta elettronica, aprire porte di ascolto e di invio. Ogni azione viene monitorata dal programma, che verifica il comportamento dell'ambiente come se fosse eseguito su un computer o su una rete non protetta, lasciando libero di agire e controllando, ad intervalli regolari, gli eventuali danni prodotti, per poi consentire l'esecuzione del programma o trasferire al centro di controllo Norman il file per un successivo controllo.

All'utilizzo pratico, il sistema si è dimostrato particolarmente efficiente, offrendo una difesa efficace e costante; interessanti si sono dimostrate le possibilità di personalizzazione della gestione, che possono rendere, di fatto, l'antivirus completamente trasparente all'utente.

• Raffaello De Masi

Norman Virus Control 5.80

PC

Prezzo: Euro 41,00 (Iva incl.) abb. un anno, 91,00 (Iva incl.) per tre anni

Contatto: Norman Data Defense Systems
Web: www.norman.com

Pro: Interfaccia agevole, ambiente di simulazione (SandBox) di concezione e implementazione originale.

Contro: Non offre alcun servizio oltre alla semplice ricerca di virus, cosa che altri prodotti simili già fanno da tempo.

Requisiti

Cpu: Pentium, Ram: 128 Mbyte (consigliati 256 Mbyte), Spazio disco: 80 Mbyte. Sistema operativo: Windows 98, Me, 2000, Xp.