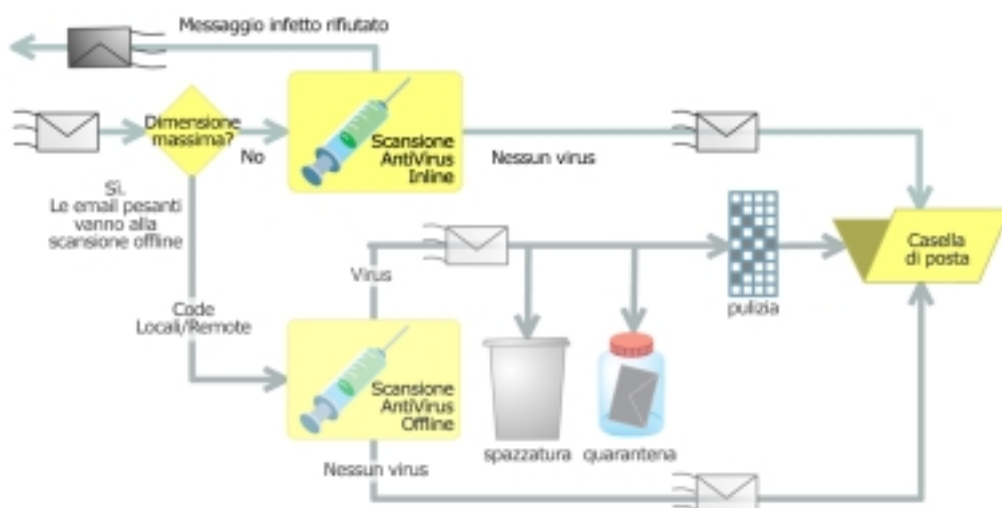


SecurityPlus for MDAemon

Da sempre i virus rappresentano una minaccia per computer, reti, informazioni e altre risorse IT. Negli ultimi anni, inoltre, ad essi si sono aggiunte numerose tipologie di **malware** come worm, spyware, adware, dialer, keylogger e altre ancora.

Programmi di questo tipo possono infettare e danneggiare software legittimo, duplicarsi fino a occupare tutto lo spazio sul disco, sottrarre dati, visualizzare messaggi pubblicitari, contattare servizi telefonici a pagamento e consentire agli hacker l'accesso alla rete aziendale. Talvolta, invece, sono solo degli inutili scherzi.

In ogni caso, **il malware costa ogni anno milioni di euro** in perdite di tempo, cali di produttività, furti e sforzi per riparare i danni, senza parlare delle responsabilità legali cui involontariamente possono andare incontro le aziende e gli utenti colpiti da software nocivo.



Fermare il malware prima che raggiunga la rete e i computer

Difendere la posta elettronica con SecurityPlus for MDAemon

Poiché l'email è comoda e facilmente accessibile, il malware si serve spesso di questo strumento per penetrare e diffondersi all'interno delle reti e dei computer aziendali.

SecurityPlus for MDAemon verifica la **presenza di virus o altro malware nei messaggi email** ed è stato studiato da Alt-N Technologies per lavorare a fianco di MDAemon.

SecurityPlus for MDAemon esamina i messaggi non appena arrivano al mail server.

SecurityPlus controlla **i messaggi e gli allegati** ricercando esemplari di codice dannoso noti o non ancora conosciuti. MDAemon di solito rifiuta i messaggi giudicati sospetti da SecurityPlus; in alcuni casi può invece accettarli e metterli in quarantena, nel tentativo di ripulirli o eventualmente cancellarli.

Dopo avere rilevato il problema, SecurityPlus

può **informare** il mittente, il destinatario, entrambi, oppure nessuno di essi.

Scansione offline e inline

MDaemon può servirsi di SecurityPlus per effettuare scansioni sia offline sia inline (cioè in tempo reale).

Le versioni di MDAemon precedenti alla 8 ricorrevano a un modulo antivirus offline denominato AntiVirus for MDAemon. Dopo che i messaggi erano stati ricevuti, venivano instradati dalle code locali e remote verso AntiVirus, che **funzionava come un processo separato**.

In seguito alla scansione effettuata da AntiVirus, i messaggi venivano rispediti alle code da cui erano stati prelevati, continuando così il loro percorso. I messaggi pericolosi o infetti potevano essere ripuliti, messi in quarantena, cancellati oppure consegnati. Mittente, destinatario e postmaster potevano eventualmente ricevere la notifica del rilevamento di un virus attraverso un messaggio email.

Oggi, invece, il mail server **MDaemon può servirsi di SecurityPlus per eseguire scansioni inline**, cioè in tempo reale. La scansione inline controlla i messaggi email **nel corso delle sessioni SMTP**. Se SecurityPlus trova un messaggio che rappresenta una minaccia alla sicurezza, MDAemon non accetta l'email o i suoi allegati. In questo modo il problema viene arginato sul nascere, prima che possa spingersi oltre.

Sebbene la scansione inline di SecurityPlus possa teoricamente ridurre le prestazioni del mail server, in pratica ha un **impatto molto basso su MDAemon**. L'impatto sulle prestazioni è limitato, tanto che AltN ha attivato la scansione inline quale tecnica antimalware predefinita per MDAemon.

La scansione offline è comunque ancora disponibile, ed è anche utilizzata per i messaggi che eccedono una dimensione specificata dall'utente, superata la quale non si applica la scansione inline.

Le firme e l'analisi euristica

SecurityPlus riconosce i potenziali virus ricercando le *firme* (o *segnature*) del malware noto. Per favorire il riconoscimento

delle minacce più recenti, SecurityPlus for MDAemon si avvale della tecnologia euristica. I metodi euristici analizzano i messaggi e gli allegati cercando di intuire la presenza di software dannosi.

Massima sicurezza con Outbreak Protection

SecurityPlus for MDAemon arricchisce le proprie capacità antivirus realizzate in collaborazione con Kaspersky Labs affiancandole alla rivoluzionaria tecnologia Outbreak Protection, una soluzione che consente di **intercettare e fermare il malware prima ancora che siano rese disponibili le relative segnature**. In questo modo Outbreak Protection rafforza la sicurezza di MDAemon anche nei confronti dei cosiddetti attacchi "del giorno zero", i più insidiosi.

Eliminare le minacce

Il plug-in SecurityPlus for MDAemon è studiato per gestire gli elevati volumi di messaggi tipicamente elaborati da un mail server. Quando affiancato alle altre misure di sicurezza di MDAemon, SecurityPlus for MDAemon riesce ampiamente a stroncare sul nascere le minacce dirette contro i computer e la rete.

SecurityPlus for MDAemon rileva e blocca i virus subito dopo la loro prima comparsa, prima ancora che siano disponibili online le relative *firme*. Per capire l'importanza di tanta tempestività, si pensi ad esempio ai problemi che ha causato un virus come MyDoom, che ha potuto agire indisturbato per mesi, spesso bloccando i mail server connessi a Internet, prima che fossero rese disponibili le segnature.

SecurityPlus for MDAemon è un valido complemento agli antivirus installati sulle singole postazioni di lavoro.

Gli antivirus installati sui PC sono utili per individuare i virus diffusi con mezzi diversi dalla posta elettronica. Per i virus che si propagano via email è infatti più logico e sicuro utilizzare SecurityPlus for MDAemon, che **blocca virus e malware direttamente sul server prima che raggiungano le postazioni di lavoro**, piuttosto che avvalersi di un semplice scanner antivirus installato sui PC client.

Installazione e configurazione

SecurityPlus for MDAemon è **semplice da installare, configurare e gestire**. Una volta installato e configurato non richiede più interventi manuali. SecurityPlus aggiorna automaticamente le signature.

La configurazione predefinita di SecurityPlus for MDAemon è tale da soddisfare la maggior parte degli utenti.

Le opzioni di configurazione consentono di **decidere cosa fare dei messaggi infetti**. Si possono rifiutare, cancellare, mettere in quarantena, cercare di ripulirli o spedirli al destinatario allegando un messaggio di avviso. È anche possibile specificare quali indirizzi email escludere dal controllo dei virus.

Manutenzione e aggiornamento

Mantenere le signature aggiornate è l'aspetto più importante della manutenzione di SecurityPlus per MDAemon. SecurityPlus for MDAemon usa le firme per identificare i virus noti. Per impostazione predefinita, SecurityPlus **ricerca quotidianamente gli aggiornamenti**, ma questa opzione è modificabile secondo le proprie esigenze. Inoltre, quando si possiede una licenza Securi-

tyPlus, ci si può iscrivere gratuitamente al servizio di segnalazione degli aggiornamenti urgenti. Quando compare un nuovo malware particolarmente pericoloso, Alt-N invia a SecurityPlus un messaggio che ne sollecita l'aggiornamento automatico.

Altre funzionalità per la sicurezza di MDAemon

SecurityPlus for MDAemon è stato studiato per una **perfetta integrazione con il mail server MDAemon**. MDAemon è leader per la sicurezza nella posta elettronica grazie alle innovazioni introdotte nella lotta allo spam, ai virus e all'uso non autorizzato dei mail server.

Tra le funzionalità legate alla sicurezza si distinguono: il meccanismo di verifica delle black e delle white list, il filtro antispam, il blocco degli indirizzi e dei domini, la crittografia, la distribuzione di certificati di sicurezza e il blocco degli utenti non autorizzati.

MDaemon può inoltre bloccare gli allegati che riconosce come portatori di malware: virus, worm, cavalli di troia (Trojan horse) e simili.

Parte integrante di MDAemon, **gli alias sono facili da creare e da amministrare**.

Principali caratteristiche di SecurityPlus for MDAemon

Configurazione

- Attivazione della scansione antivirus.
- Esclusione dei gateway dalla scansione antivirus.
- Rifiuto dei messaggi infettati (se è attiva la scansione inline).
- Impostazione degli indirizzi sicuri.

Azioni dello scanner

- Cancellazione degli allegati infetti.
- Messa in quarantena degli allegati infetti.
- Pulizia degli allegati infetti.
- Cancellazione dei messaggi infetti e degli allegati.
- Messa in quarantena dei messaggi infetti e degli allegati.

- Ignorare i messaggi infetti.
- Messa in quarantena dei messaggi di cui non è possibile effettuare la scansione.
- Aggiunta di un messaggio di avviso ai messaggi infetti.

Aggiornamento delle signature

- Iscrizione al servizio di segnalazione di aggiornamenti urgenti.
- Aggiornamento immediato delle signature.
- Visualizzazione del report di aggiornamento.
- Configurazione del proxy per la connettività
- Programmazione degli aggiornamenti automatici.

Achab S.r.l. - Piazza Cinque Giornate, 4 - 20129 Milano
Tel: 02 54108204 - Fax: 02 5461894 - <http://www.achab.it>
Informazioni commerciali: sales@achab.it
Informazioni tecniche: supporto@achab.it