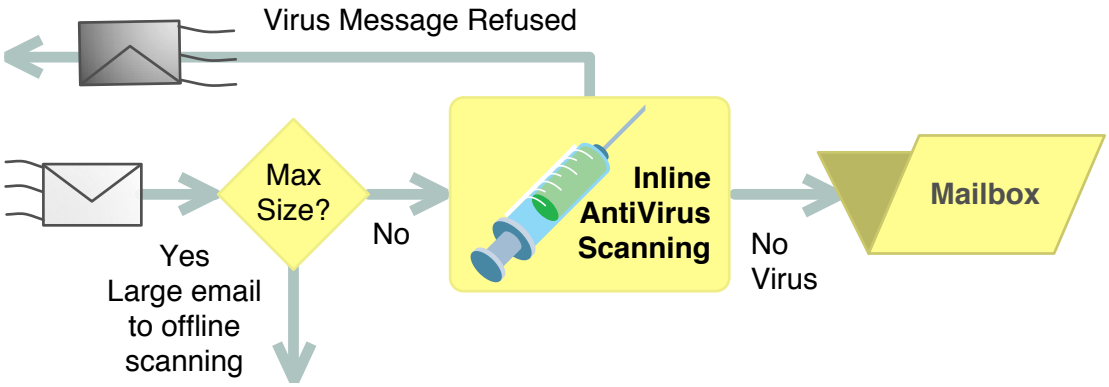
MDaemon Benefits

alt-n technologies
Helping the World Communicate!

Inline AntiVirus Scanning for MDaemon

In addition to their direct damages, viruses cause peripheral losses by wasting time and resources. This happens because most AntiVirus software scans files after they enter your email server or show up on your personal computer.

While scanning files after their arrival is better than no protection at all, this method is similar to dragging in a trojan horse and waiting to see what pops out. A more effective solution blocks the intruders at the door. After all, malicious software cannot cause any harm unless it gets inside.



Detecting and rejecting viruses with the least amount of time and effort

Refusing Virus-Infected Emails

AntiVirus for MDaemon provides virus detection services for Alt-N Technology's MDaemon email server. Beginning with MDaemon 8, the email server can now use AntiVirus to scan messages *inline* during each SMTP session.

Inline scanning effectively stops most malicious software at the email entrance to your network. When AntiVirus detects a message corrupted with a security threat, MDaemon refuses to accept the email or its attachments. Doing this stops the trouble before it starts.

Increased Security, Reduced Risks

Refusing entry of email-borne malware strengthens your security and saves you the risk and work of cleaning up virus problems internally. It reduces and often eliminates the possibility of electronic trespassers causing any damage.

Designed specifically to work with AntiVirus for MDaemon, inline scanning looks inside each message plus any attachments for both known and suspected interlopers.

Inline scanning protects your users and your network by closing the door on messages polluted with viruses. They never enter the main flow of email in your server.

Inline AntiVirus protection deployed on your email server is your first line of defense against software invaders.

Reducing Waste with Inline AV

When an organization permits contaminated emails to enter their network, they assume responsibility for neutralizing the messages and notifying all concerned parties. On the other hand, refusing to accept corrupted messages returns them to the sender for handling.

In the past, MDaemon worked with AntiVirus by using it only as an offline operation. Offline virus processing receives all messages. It sends them from the local and remote queues to AntiVirus, which runs as a separate process.

After the security software scans the messages, it returns them to their queues to continue process-

ing. Some messages are marked as security offenders. Typically, infected emails are cleaned, quarantined, deleted or delivered. Also, the sender, recipients and server postmaster receive email notifications concerning the virus transactions.

All of this work consumes computing resources, plus the efforts of the people involved. There is also the chance of a virus-infected email to accidentally become active on a network.

This waste of time and resources, plus the risk, does not occur with inline scanning. For example, before deploying inline scanning, one administrator for multiple domains was receiving more than 500 virus-cleaning notifications each day. By using inline scanning to refuse contaminated messages, this number has been reduced to zero. Eliminating these messages unclutters the *postmaster* inbox, making other messages easier to find.

Inline Scanning as MDaemon's Default

Inline scanning is an MDaemon feature. It uses the current regular version of AntiVirus for MDaemon. While it can in theory slow down email server performance, inline scanning provides rapid throughput in MDaemon. The effect on performance is limited enough for Alt-N to enable the inline option as the default AntiVirus scanning method for MDaemon.

Offline scanning is still available optionally. It is also used for messages exceeding a user-specified size.

Scanning Operations Summary

As with offline scanning, inline scanning recognizes would-be invaders by looking for the *digital signatures* of known viruses.

To help detect newly released hazards, it also uses heuristic technology, the ability to analyze messages and attachments for threat-like patterns.

The most important part of accurate scanning involves keeping your signature definitions file current. AntiVirus for MDaemon uses the signature file to identify known software threats. By default, AntiVirus checks daily for updates. You can alter this to match your needs.

Also, with a licensed copy of AntiVirus, you can sign up for free *urgent update* notifications. When a new serious threat appears, Alt-N sends an emergency update notice to your AntiVirus, which then automatically updates itself with the new information.

More complete information about general AntiVirus operations is in the *MDaemon AntiVirus Benefits* article.

Ongoing Development

Inline scanning is the most recent development in MDaemon's ongoing fight to reduce the amount of viruses getting through to email users.

Continual development is necessary because the creators of viruses also regularly devise new methods of spreading their chaos. Some virus writers are skilled at building in stealth and complexity. Fighting viruses requires a continuing and comprehensive strategy, nothing as simple as loading one type of software and forgetting about it forever.

Also, while AntiVirus security on MDaemon helps detect and stop threats carried by email, it should be viewed as only one of several defenses against malicious programs and scripts. AntiVirus for MDaemon works alongside desktop virus protection applications to fight software threats. It does not replace the desktop security tools. It forms the front line of AntiVirus defense.

Alt-N Technologies, Ltd.
2201 East Lamar Blvd, Suite 270
Arlington, Texas 76006
Phone: (817) 525-2005
Fax: (817) 525-2019
http://www.altn.com