A complete virus-protection solution must cover all entry points of your company’s network. The most likely entry and propagation points are listed below. (For this article, we assume that your company is using GroupWise. If your company is using Microsoft Exchange or another groupware solution, you will need to identify the entry points for that solution.)

- Software or web pages that users access on the Internet
- Removable media (such as disks or CDs)
- Files attached to an e-mail message that users access with the GroupWise 32-bit client
- Internet e-mail
- GroupWise WebAccess client

To effectively eradicate viruses that propagate via the first two entry points, you must use a combination of workstation- and server-based virus-protection software. If you are not already running virus-protection software on all of your company’s servers and workstations, you should make plans to purchase this software now. When making your purchasing decision, you should factor in your company’s GroupWise system. (For more information, see “Workstation- and Server-Based Virus-Protection Software and Its Relationship to GroupWise.”)

To effectively eradicate viruses that propagate via the GroupWise entry points, you should follow the guidelines outlined in this article.

PROTECTING THE POST OFFICE AGENT (POA)
Currently, no virus-protection software is available for the GroupWise POA. If you are not running virus-protection software on workstations, users can propagate viruses through e-mail to other users in the GroupWise system.

PROTECTING THE MESSAGE TRANSFER AGENT (MTA)
Beginfinite (www.beginfinite.com) offers GWAVA (GroupWise Anti-Virus Agent) virus-protection software for the GroupWise MTA. GWAVA integrates with most existing server-based virus-protection software.

GWAVA is a NetWare Loadable Module (NLM) that works in conjunction with the GroupWise MTA. Because GWAVA protects the GroupWise MTA, GWAVA prevents users from sending viruses to users in other post offices. We have implemented GWAVA at customers’ sites and have been surprised at the results. For example, Tay recently implemented GWAVA for a customer and found that GWAVA filtered 5,600 instances of a virus in a two-hour period.

PROTECTING THE GROUPWISE INTERNET AGENT (GWIA)
As you know only too well, Internet-propagated e-mail viruses are the biggest threat to your company’s network. The best way to stop these viruses is at the entry point from the Internet. The GWIA is a common entry point into your GroupWise system.

Virus protection providers usually take one of the following approaches to providing virus-protection software for e-mail:

- Virus protection at the MTA for the GWIA’s domain
- GWIA third-party queue integration
- Simple Mail Transfer Protocol (SMTP) mail hosting with a virus scanner

Protecting the MTA for the GWIA’s Domain
GWAVA is one example of a product that protects the MTA for the GWIA’s domain. The GWAVA agent takes messages that are sent to the GWIA’s domain and submits them to server-based virus-protection software. After the virus-protection software scans the messages for viruses, GWAVA allows the messages to be processed. What sets GWAVA apart from other virus-protection software is that it is NLM based. As a result, GWAVA is fast.
When the GWIA receives an outgoing message from the MTA, the GWIA converts the message into ASCII format. The GWIA then typically spools these files to its internal SMTP daemon. You can configure the GWIA to spool these files to another directory, which becomes a third-party integration queue. You can then have the virus-protection software scan the files in this queue for viruses. The virus-protection software must then move the files to an input directory for the GWIA.

Many virus-protection products are written to work in this way for most e-mail systems. For example, you may want to check out the following products:

- Integralis Inc.’s MIME sweeper (www.integralis.com)
- Network Associates Inc.’s WebShield (www.networkassociates.com)
- Symantec Corp.’s Norton AntiVirus for Internet E-mail Gateways (NAVIEG) (www.symantec.com)
- Trend Micro Device Inc.’s InterScan E-mail VirusWall (www.antivirus.com)

Two products are specifically designed for the GWIA’s third-party integration queue:

- Guinevere (www.indecon.com/guinevere)
- GroupWise Footnote (www.stack.co.uk/groupwise_footnote.htm)

Guinevere ingeniously leverages desktop virus-protection software to scan GroupWise messages. With the GWIA’s configurable third-party queue, Guinevere scans the GroupWise messages and then moves them to the input queue for the GWIA. Guinevere requires a Windows NT or Windows 2000 workstation.

Footnote is supposed to work in the same way that Guinevere works. However, neither of us have any experience with Footnote.

For more information about configuring the GWIA for these solutions, read the Technical Information Document (TID) at http://support.novell.com/cgi-bin/search/tidfinder.cgi?TID=10011919.

SMTP Mail Hosting

Mail hosting means that the GWIA is not sending or receiving SMTP mail to or from Internet SMTP hosts. Instead, another SMTP device, a host, handles the SMTP mail for the GWIA. The host receives incoming e-mail messages from the Internet. Virus-protection mail hosts scan the messages for viruses and then forward the messages.
You can then configure the GWIA to relay outgoing e-mail messages to the mail host. The mail host then scans these messages for viruses before sending the messages to the Internet.

You can maintain virus-protection hosts at your site, or you can have an application service provider (ASP) provide the virus-protection host for you.

**PROTECTING GROUPWISE WEBACCESS**

GroupWise WebAccess changes the face of virus protection at your company's site. The biggest concern is that users working at home or at other locations outside of your control may be able to send virus-laden attachments into your company's network.

To protect against viruses spreading via the GroupWise WebAccess client, you should understand how GroupWise WebAccess works. The web-server servlets for GroupWise 5.5 Enhancement Pack and GroupWise 6 WebAccess place attachments in a directory on the file server where the web server is running. (On a NetWare server, the default location for this directory is SYS:NOVELL\WEBACCESS\TEMP.) Because the attachment files remain in their native format and are stored in this directory for a short period of time, server-based virus-protection software can continually scan this temporary directory to detect viruses.

We have one caution, however: You should understand how your virus-protection software works before you assume this software can effectively scan this temporary directory. For example, one of our customers we work with has tested its server-based virus-protection software with GroupWise WebAccess. This customer found that its server-based virus-protection software did not catch viruses in the ...\TEMP directory when a virus-laden document was attached to an e-mail message.

The customer's server-based virus-protection software seemed to rely on files being placed on a server via a NetWare client. In the case of GroupWise WebAccess and a web server, a file does not pass through a NetWare client.

The Novell customer then tested Computer Associates's InnoculateIT 4.5 for NetWare, which was able to detect viruses sent via the GroupWise WebAccess client. This customer observed the following: If a user uploaded several files and one of the files contained a virus, the file with the virus never got through. The customer noticed, however, that the other files that were uploaded with the message may or may not have gotten through to the recipient. That's not so good, but, hey, at least the virus didn't get through!

**REACTIVE SOLUTIONS FOR ELIMINATING E-MAIL VIRUSES**

If a virus manages to infiltrate the GroupWise message store, you should use GWCHECK with the ITEMPURG command to eliminate the virus. The instructions for using GWCHECK and the ITEMPURG command vary, depending on which version of GroupWise you are using. If you are running GroupWise 5.5 or GroupWise 5.5 Enhancement Pack, you will find some well-written documentation about ITEMPURG at http://support.novell.com. Search the knowledgebase for document 10052682, or simply search for ITEMPURG.

If you are running GroupWise 6, the GWCHECK interface now includes a field for special commands such as ITEMPURG. What's even better is that these special commands can be issued from ConsoleOne or the standalone GWCHECK (GWCHECK.EXE).

**Note.** Do not use the standalone GroupWise 6 GWCHECK on a GroupWise 5x post office. Although you can issue GWCHECK jobs on a GroupWise 5x post office from ConsoleOne, the GroupWise 5x POA ignores the features that are new to GroupWise 6.

For the fastest execution of the ITEMPURG command, you should issue the GWCHECK-Mailbox/Library maintainance job from ConsoleOne and allow the GroupWise 6 POA to perform the GWCHECK job. Highlight a GroupWise post office or user in either the GroupWise view or the eDirectory browser view, and select Tools|GroupWise Utilities|Mailbox/Library Maintenance. To run the ITEMPURG command on a post office, you should use the following commands:

```
GWCHECK-Mailbox/Library maintainance

ITEMPURG
```
Note. The matching algorithm works from left to right and does not match portions in the middle of the string or at the end of the string. The algorithm looks for matches starting with the left-most part through the first 27 characters of the string. Spaces in the string also count. The matching algorithm is not case sensitive.

For example, suppose you want to purge messages with "ILOVEYOU" in the subject line. Both of the following show the correct syntax for the Support options field in the ITEMPURG command:

```
itempurg=ilovey
or
itempurg=ILOVEYOU
```

If the subject line includes other text such as "Fw: ILOVEYOU" or "Re: ILOVEYOU", you must issue a separate GWCHECK/ITEMPURG job. In this case, the Support options field should read as follows:

```
itempurg=re: iloveyou
```

You then click the Run button. If you are running GWCHECK from ConsoleOne, the Mailbox/Library Maintenance-GWCHECK job is sent to the POA to perform. If you are running the stand-alone GWCHECK, the Mailbox/Library Maintenance-GWCHECK job executes at the workstation.

GWCHECK creates a log. If GWCHECK finds anything that matched the ITEMPURG command you specified, the log includes text similar to the following:

```
1 FOLDER_RECORD (Universal Inbox)
  282 ITEM_RECORD check
    - Item matches subject "ILOVEYOU"
    - Item 282 purged successfully
```

Problem 87 - Special Cleanup
Successfully deleted: "ILOVEYOU"

If GWCHECK does not find anything that matches the ITEMPURG command you specified, the log does not contain any evidence that you even issued this command.

Tip. You can make the GWCHECK job run even faster by using the PA BSkip command before the ITEMPURG command. If you use the PA BSkip command, GWCHECK will not check users' personal address books as it usually does when running a contents check and fix. To include the PA BSkip command, use the following syntax in the Support options field:

```
pabskip, itempurg=iloveyou
```

CONCLUSION
Virus threats are expected to get even worse in the future. Although GroupWise isn't impacted by viruses nearly as much as Microsoft Outlook and Exchange, you still need to implement a proactive virus protection solution for your company's GroupWise system. With the heavy proliferation of the Outlook client and its ability to access MAPI-compliant messaging systems, such as GroupWise, viruses that are propagated from within your GroupWise system are far more likely than they were in the past.


Danita Zanré has been using GroupWise since 1989, when its predecessor was known as WordPerfect Office 2.0. She is experienced in all aspects of GroupWise, from design and installation to training. Danita is one of the primary consultants responsible for the day-to-day operations of Caledonia Network Consulting and is the coauthor of the GroupWise 5.2 Administrator's Guide, GroupWise 5.5 Administrator's Guide, and GroupWise 6 Upgrade Guide. (For more information, visit www.caledonia.net.) Danita is also a sysop on the Novell Support Connection (http://support.novell.com).