How MWL fights ethreats

MicroWorld Winsock Layer (MWL) is a radical technology that fights viruses and other threats from a new perspective. Developed by MicroWorld Technologies Inc., MWL blocks threats at the Internet gateway itself and does not allow them to enter your system.

This article discusses features of MWL and explains how it does its anti virus and content security tasks, efficiently and quietly.

What is MWL

When you connect to the Internet, you do so through the Windows Socket (Winsock) layer. The Winsock layer is an integral part of the Windows operating system. The layer acts as an interface between your computer and the Internet. It does its work very efficiently and you can surf the net, download programs etc unhindered. But it never distinguishes between a virus infected file and a clean one or between Spam and genuine mails.

Our MWL layer sits on the Winsock layer. It checks and analysis all traffic between your system and the Internet. All e-mails, attachments, downloads, etc are scanned before they enter your system. If any virus or harmful content that violates your security policy is detected, such traffic is blocked at the gateway itself and not allowed to enter your system.

Our anti-virus and content security applications are built on the MWL technology. Our applications have a vast database of all known viruses and other threats. MWL ensures that any files with these known threats are barred from entering your system.

What edge has MWL got over our competitors

Products made by other manufacturers do not have the intelligence to recognize and stop threats from entering your system. They allow them entry, permit them to infect your system and then wait for the obsolete Anti-Virus software you have installed to identify them. IF and when these threats are identified, then the obsolete Anti-Virus software tries to disinfect the files.

The whole process is subject to jargon like 'possible scenarios' ' threat perception' etc. You lose priceless data and spend valuable time in removing a threat, which should not have been allowed into your system in the first place and end up entertaining your staff, with your frenzied 'containment procedures'.

MicroWorld endorses the timeless proverb "prevention is better than a cure". Stop the threat from entering your system. There is no way a threat can bypass the MWL technology and compromise your system. The first time you install our product, our Anti-Virus software thoroughly checks your system and removes all known virus. If new or unknown threats are discovered, you can delete or quarantine these files. Mail us a copy of the file and we will get back to you with possible means to tackle them.

How does MWL work

MWL sits on the Winsock layer and all traffic must pass through it before the traffic is allowed into your system. MWL disassembles data packets of the traffic and decodes HTTP, Chat and FTP objects. It acts like a 'transparent gateway' on your system rather than like a 'proxy gateway' which other products employ.

All objects are scanned for viruses and other threats. If the traffic is found to be benign, then it is reassembled and allowed inside your system. If any malignant threats are present, they are detected and the traffic is blocked at the gateway itself.

When e-mails with infected attachments are detected, our anti virus applications allow you to auto clean, delete or quarantine them.

Figure 1 shows how MWL protects your system.

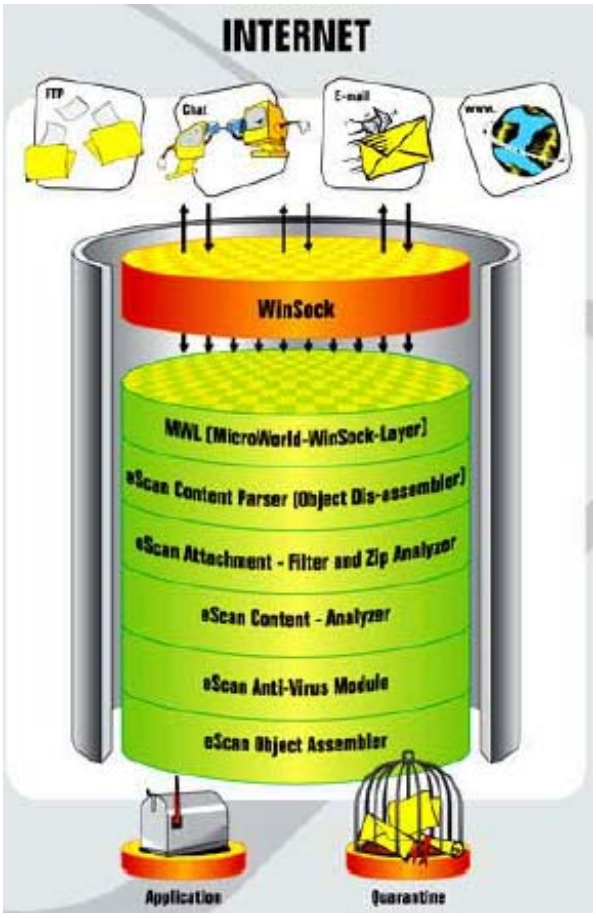

Figure 1. How MWL protects your system

Let me explain the difference between a 'transparent gateway' and a 'proxy gateway' with an example:

When you receive a mail from hotmail.com, the mail server on hotmail.com identifies itself to your mail server using its IP address (65.54.167.5) and your mail server accepts the mail.

If a 'proxy gateway security' is present on your machine, then the IP address of hotmail.com (65.54.167.5) gets "hidden" from your mail server. But if a 'transparent gateway' like MWL is present, the transparency is maintained and your mail server gets to see the actual IP address.

Your mail server administrator can set localized security policies on the mail server itself.

What happens when MWL is not there

The answer is obvious; you are unprotected – like going out in the driving snow, without a stitch on.

Figure 2 shows what happens to your mail server when it is without MWL protection.

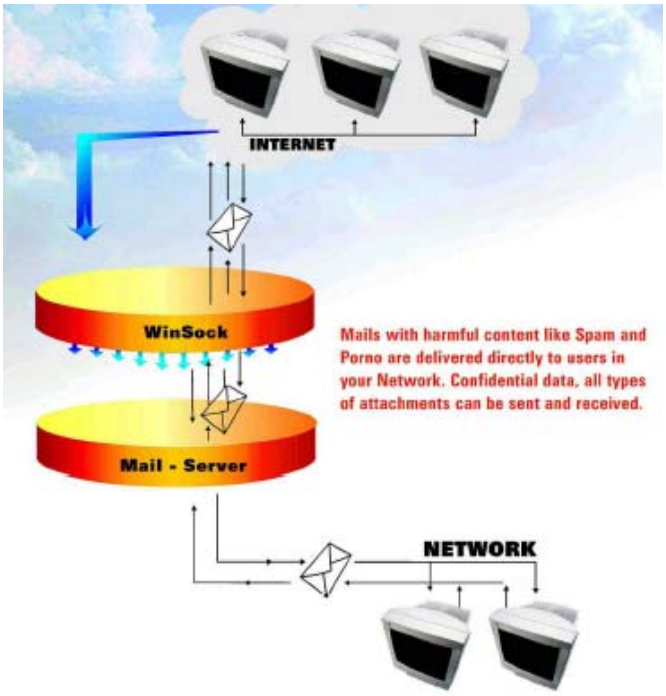

Figure 2. Your mail server without MWL

Our Satisfied Clients

We sell our products across the globe with over 10,000 partners and resellers. We protect desktops, LANs, WANS, SOHO, mail servers, etc. The list of our satisfied clients is a literal who's, who of the IT world.

We provide 24x7 online support through chat and e-mails. Given below are some thank you mails from people we protected and served.

"Stephen Hartley" shartley@netability.com.au

We have been using eScan (www.mwti.com) since October last year when several of my clients got "hit". Not one of them has been infected

with a single virus since then - whether the virus signatures were up to date or not! Let's face it, most viruses these days are e-mail borne, so if you are scanning incoming messages and blocking bad attachments, 99 percent of your troubles will be solved. Around 80 percent of the viruses coming into my machine (but being blocked!) are coming from machines supposedly protected by Norton's Antivirus - says something about that product me thinks! The content management is a real bonus and simple to manage!

Stephen Hartley

NetAbility

Brisbane, Australia

"Rovic" rovic@hom.com.au

Viruses often Have Many Aliases ... .eSCan Uses Kaspersky Virus Defs ..so Have NO FEAR ..they are all there but often with different names.

eScan remains the BEST AV package I have tried ands I have tried MANY!! ...and I dont even work for them!!...:-)

Rovic

For a full list of satisfied customers, please visit:

http://www.mwti.net/antivirus/escan/escan_commendations.asp

It gives us immense satisfaction when we get thank you mails from small business and home users. These folks do not have the means to invest in expensive solutions. Protecting the vulnerable is our goal.

To find out how MicroWorld can help you fight eThreats, visit http://www.mwti.net/