# Global Information Assurance Certification Paper

# REMOTE CLIENT WORKSTATIONS:
# The Neglected Nodes

**by**
**John J. Dwyer**



**SANS Security Essentials**
**GSEC Practical Assignment**
**Version 1.4b**
**Option 1**
**Submitted December 6, 2003**

# Remote Client Workstations: The Neglected Nodes

## Introduction

A network security infrastructure is only as strong as its weakest link. The perimeter of a network can be secured with firewalls, packet-filtering routers, and mail servers that can block dangerous attachments. However, remote end-point hosts are often overlooked when setting up a network security infrastructure and this poses a threat to overall corporate security. Remote endpoints represent the least protected area of the network. This paper will examine some of the vulnerabilities and types of attacks that could be launched against these unprotected remote hosts before they even connect to the company network. Their subsequent connection to the network could negatively affect the corporate network. Also presented will be some countermeasures to combat these threats and several of the available vendor solutions that would strengthen security for these "neglected nodes".

**Remote Client Workstations: The Neglected Nodes**

Three major vulnerabilities that remote workstations may demonstrate are a lack of up to date security patches, a lack of intrusion detection capability, and anti-virus software that either is not installed or does not have the latest definitions. In addition, services can be turned off by hackers or end-users and unauthorized programs such as peer-to-peer file-sharing applications like KaZaA, Napster, Bear Share, etc…. could be installed. Because of this lack of safeguards and centralized control, the remote hosts may already be infected with a virus, Trojan, worm, spyware or some other type of malicious code before they even connect to the corporate network. Subsequently, if these unprotected end-point workstations are then connected to the network through a VPN or locally by a traveling employee or a visiting consultant, there could be a rapid spread of the malicious code among unpatched workstations.

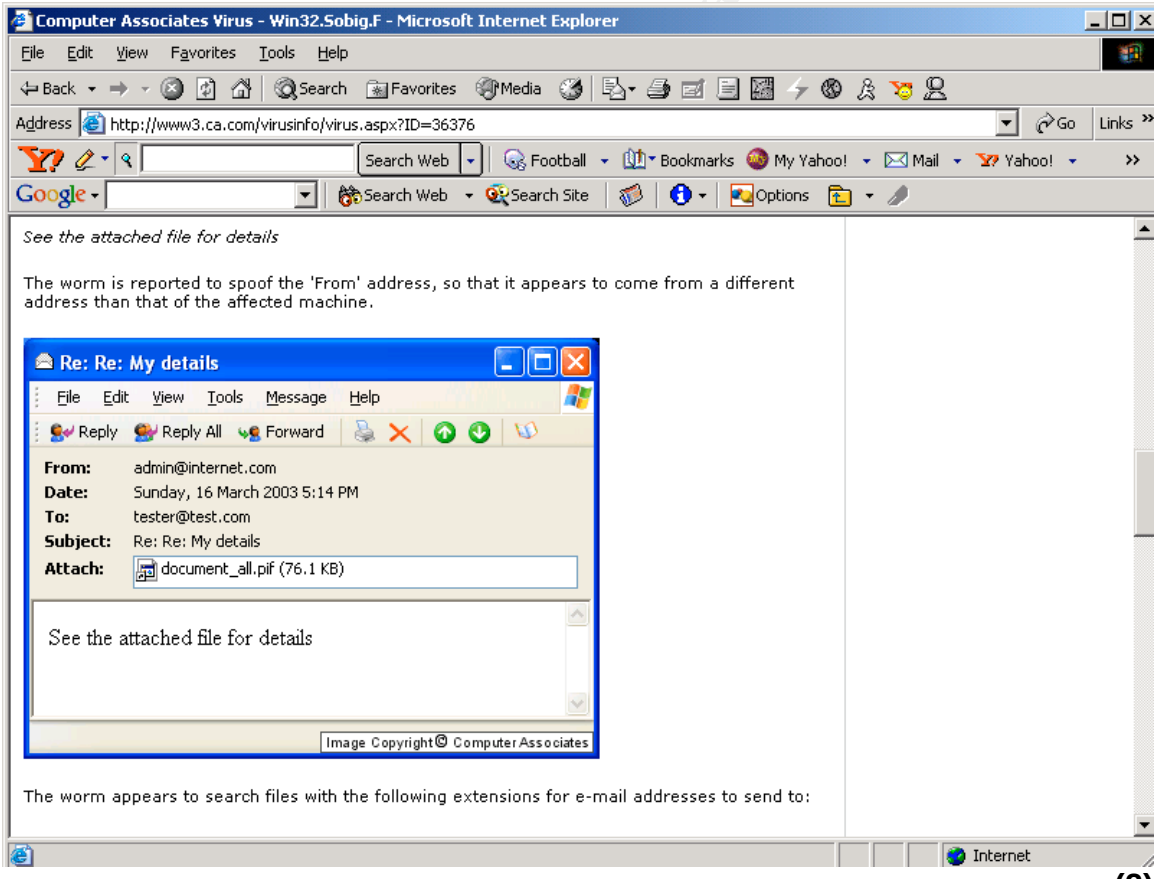
This type of breach could result in loss of confidentiality, a loss of data integrity and unavailability of data due to systems downtime along with the cost of recovering the affected systems. An example of this type of malicious code was the MS-Blaster. Worm, which exploits a vulnerability of the Remote Procedure Call (RPC). W32.Blaster.Worm is a worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. The worm also attempts to perform a Denial of Service (DoS) on the Microsoft Windows Update Web server (www.windowsupdate.com). This is an attempt to prevent a user from applying a patch on their computer against the DCOM RPC vulnerability. This worm causes a loss of user productivity, increases helpdesk calls and can affect network bandwidth negatively through these Denial of Service attempts. Therefore, even if the network administrator were filtering port 135 on the firewall, this would not stop the spread of this worm on the LAN because an infected laptop that is hooked up to a local node would not have to go through the firewall.

- An infected computer may receive the following error message:

  The Remote Procedure Call (RPC) service terminated unexpectedly.
  The system is shutting down. Please save all work in progress and log off.
  Any unsaved changes will be lost.
  This shutdown was initiated by NT AUTHORITY\SYSTEM.

  **(1)**

A second example of malicious code that could take advantage of an unsecured host end-station is the Sobig.F worm. This worm infects machines through an e-mail attachment with a .SCR or .PIF extension. Thus, if the remote workstation receives email through another source beside the corporate email server, it may receive an email with this type of attachment. If the user opens the attachment, the worm will infect the computer. It will then make a number of outbound connection attempts to a master server to download a backdoor Trojan or to upgrade itself. After that, the worm spreads itself by using open network shares and its own SMTP (Simple Mail Transport Protocol) engine to send e-mails to addresses taken from the infected computer's hard drive. This worm results in both a loss of confidentiality due to the backdoor Trojan and disrupted business services. Therefore, even if the corporate email server is blocking this type of attachment, an unsecured remote host can introduce this worm through open network shares. Below is an example of the Sobig.F attachment.




**(2)**

Most corporate security efforts are directed to network perimeter devices, such as firewalls and corporate servers. This is because these measures will have a greater impact with a lesser amount of cost and effort. It is easier to set up a firewall, block attachments at the e-mail servers and apply security patches and harden all your corporate servers than to manage and control hundreds if not thousands of workstations both locally and remotely. With limited staff and the almost daily release of security patches, it is difficult to apply these required patches automatically to all of the servers let alone all of the workstations. Remote end-points present additional security problems. Besides not having the latest security patches applied, they also lack intrusion detection with centralized logging, firewall protection, and automatic anti-virus update capabilities.

**Countermeasures** that could make these host end-stations more secure are:

a. Anti-virus software with automatic updates
b. Personal firewalls with centralized reporting
c. Automatic security patch updates
d. Enforceable security policies

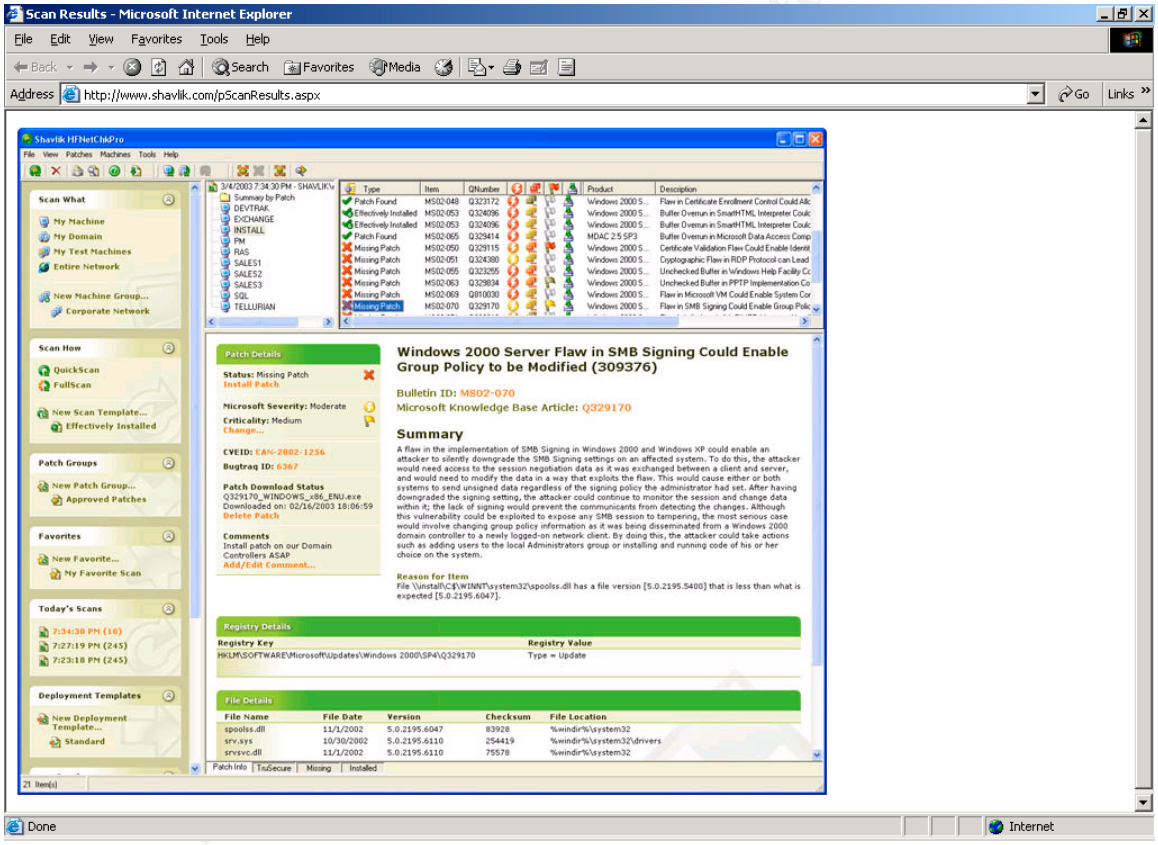
These countermeasures should be automatic not requiring or permitting end-user intervention. End users sometimes forget to update their virus definitions or try to turn off security services while installing unapproved software. If security patches are not up to date or the virus definitions are not current and the machine does not comply with the corporate security policy, then the machine should be isolated from the main network until the current patches and virus definitions are updated, and the machine is in compliance. These counter measures could come from one integrated package or could be combined from various vendors to protect the remote host

A relatively new security market for remote end-point security developed in 2001 as security service vendors began offering products to this segment. The Yankee Group estimates that the remote end-point security products and services market was approximately $60 million in 2002 and is projected to exceed $520 million by 2007. The Yankee Group also predicts that the Host Intrusion Prevention market will increase greatly by about 150 percent in 2003. The Yankee group report provides an introduction to secure end-point services, discusses current vendor offerings and suggests the future directions for this area. **(3)**

**Commercial products that address remote host security:**

### 1. Shavlik HFNetChk Pro 4.0

HfNetChkPro 4.0 can automatically analyze and deploy required security patches after scanning the network. It allows one to view detailed information about each patch and has links to external patch data, including BugTraq ID and Common Vulnerabilities ID (CVE ID). It uses the same scanning engine that Microsoft uses in its "Microsoft Baseline Security Analyzer" (MBSA). HFNetChk and MBSA were developed by Shavlik Technologies. **(4)**




Above is a screen shot of HFNetChkPro GUI **(5)**. One can scan a whole subnet at once or a single host. Required patches can be deployed to the hosts from this central console.

Shavlik also has a free version called HFNetChkLt 4.0. This product can also scan network computers for the required security patches. However, one is limited to deploying only two security patches per machine at a time. A reboot of the patched computer would then be required. In addition, only operating system patches can be deployed from this light version. Security patches for Internet Explorer, Internet Information Server, Microsoft Office, and Java can only be deployed from the Pro version, although it will list the appropriate links to the security patches and CVE ID's. Still, the light version is a good tool even if one simply wants to see the security patches that are required for a network.

Scans can be scheduled from the console and one can create a baseline patch template that is right for a particular organization. With the frequency of released security patches, it is important to have a tool that can automate the security patch scanning and deployment. While this product does a good job of taking care of required security patches, remote hosts still would have additional vulnerabilities that would have to be addressed by other security products such as some type of personal firewall, intrusion detection with centralized logging, and security policy enforcement.

## 2. Zone Labs "Integrity 4.5"

Zone Labs end point security system for Windows computers are made up of two pieces: Integrity Server and Integrity Client. The Integrity client protects the desktop using a combination of three security components:

- A stateful desktop firewall that blocks unsolicited Internet traffic while allowing valid traffic initiated by the client. The effect of the firewall is to put the computer in "hidden" mode, making it invisible to other machines on the Internet.

- Application control, which manages the rights of local applications to access the Internet. This prevents malicious applications from transmitting information over the network. This could prevent the remote host from becoming part of a Distributed Denial of Service Attack (DDoS).

- MailSafe email protection, which guards against potentially harmful email attachments**.**

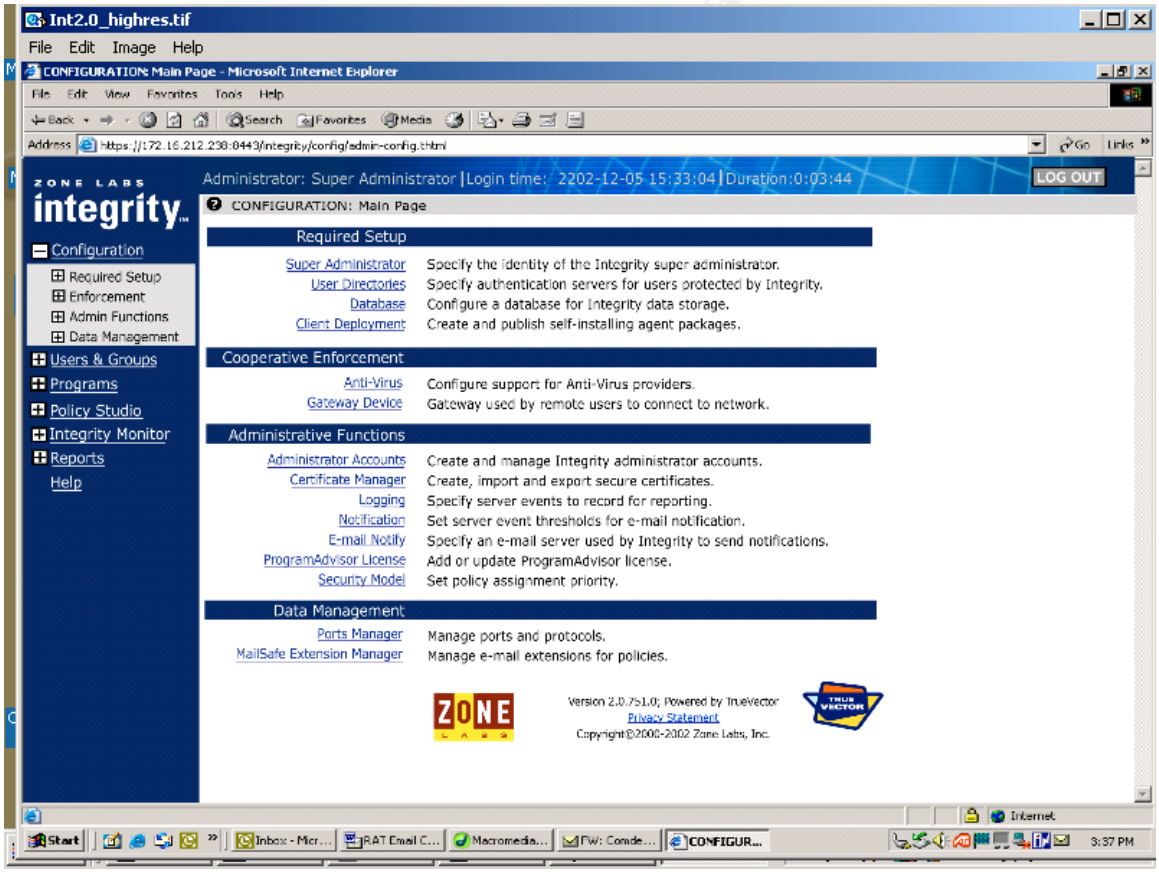
**(6)**



The Integrity client can be transparently deployed with your existing network solution; including Microsoft's SMS, IBM's Tivoli, or HP's Openview.

The client software implements endpoint security for each client based on policies provided by the Integrity server. When the Integrity client starts up it begins enforcing the appropriate disconnected policy before it even connects to the Integrity Server.

Integrity Server uses a standards based security policy to enforce endpoint security policies on all computers that access the network, whether from a remote node or from within the network. An important centralized management feature is policy templates that can be customized. There are several predefined rule sets for common enterprise security setups to get started with. These templates can further be refined to fit an organization's needs. Integrity Server supports Windows® 2000 and Windows 2000 Advanced Server systems while Integrity clients run on Windows 95 (OSR2), 98SE, 2000 Pro SP4, NT 4.0 Workstation SP6a and XP Professional machines. The Integrity Server console is shown below.



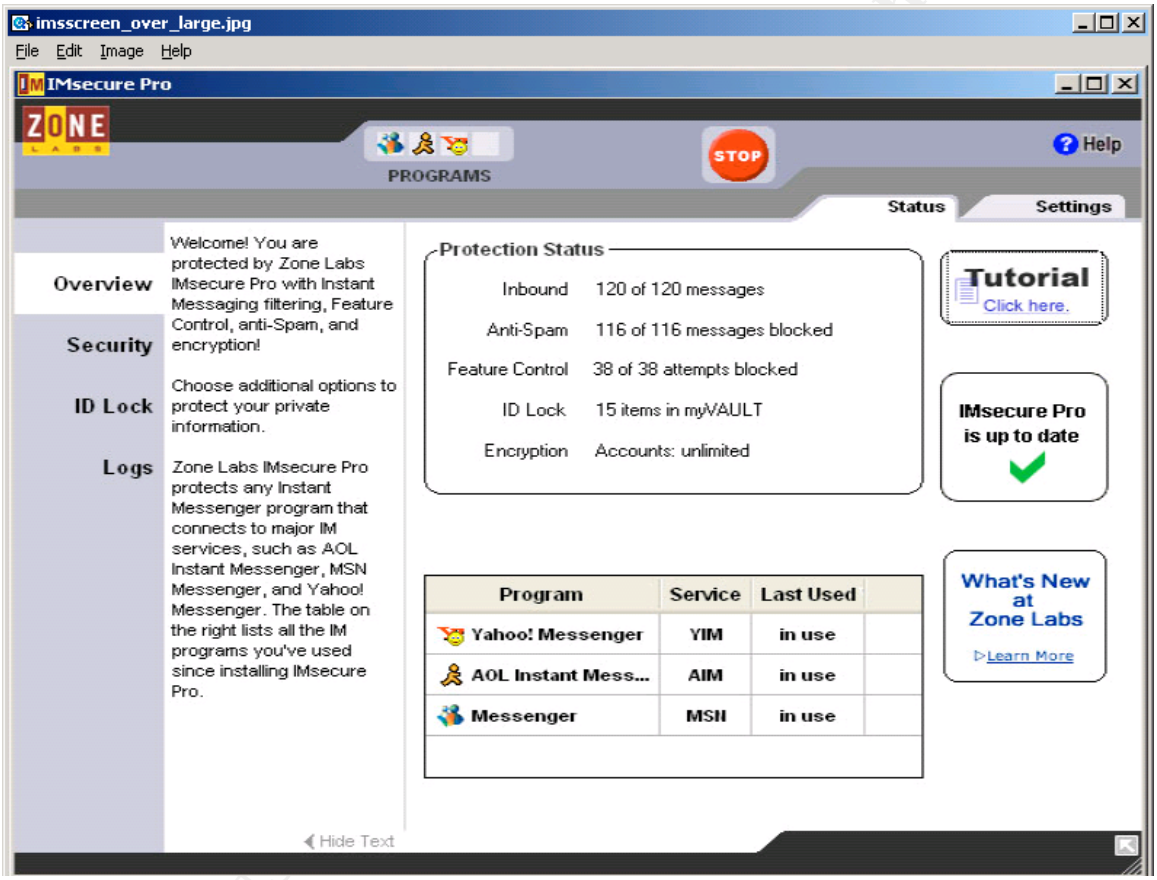

**(7)**



Zone Labs and Nortel now support "Cooperative Enforcement Technology" for Contivity's VPN's, ensuring that only policy compliant endpoints

can access the corporate network. It allows administrators to enforce network access prerequisites for remote nodes to ensure that:

- Patches and service packs that should be deployed are actually installed.
- Antivirus is running and current.
- Authorized applications are present.
- VPN clients are the correct version.




**(8)**

Shown above is the **optional** Instant Messaging security module that is available at an extra cost per seat. Integrity 4.5 includes an optional module to secure computers from vulnerabilities introduced through any client that accesses AOL, MSN and Yahoo! public IM services. Integrity 4.5 enables central management of encryption for instant messages, content filtering, usage controls, unsolicited communication blocking, as well as usage and event reporting.



### 3. PestPatrol Corporate Edition

Provides a combination of tools to combat threats from hacker tools, Trojan horses, key loggers and spyware. Its core components are comprised of:

- PestPatrol CL – the command line on-demand scanner. It is the core of the PestPatrol solution. It can be invoked by a login script. If a user attempts to log in to the network with an infected machine, the administrator will be notified. PPCL provides a complete scan of the client PC at logon.

- PestPatrol MemCheck – the active memory scanner that is designed to provide real time protection. It provides protection against the execution of a pest downloaded sometime after the initial logon and before the next one.

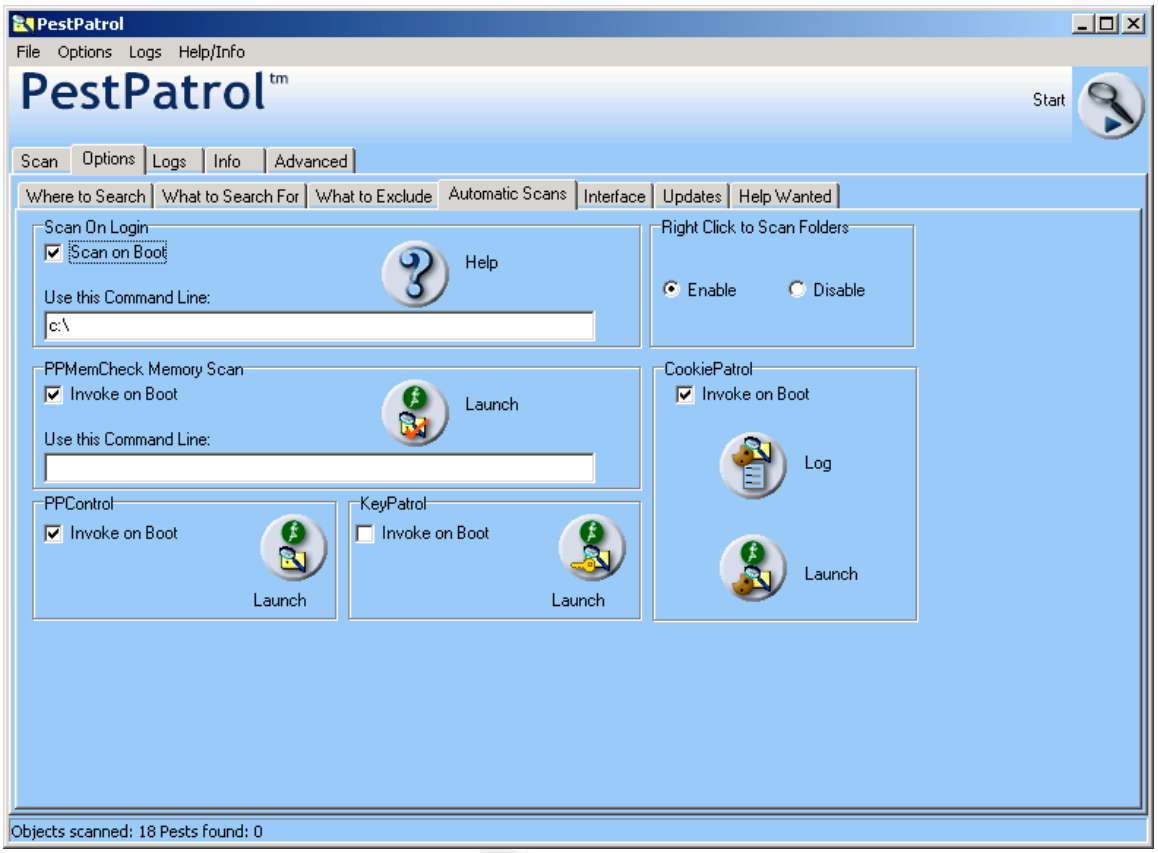
- Cookie Patrol – will automatically detect and get rid of spyware cookies as soon as they arrive on a user's machine. No user intervention is required.

- Key Patrol – detects key loggers.

- PestPatrol Updater – to ensure all components and .dat files are up to date. Used on the PDC and BDC from where the login script is run.

- PestPatrol GUI – the optional graphical user interface. May be installed on a server or run from a client machine. Can be used by system administrators to review the master log and the quarantine folder. Shown below is a screenshot of the PestPatrol GUI.

**(9)**



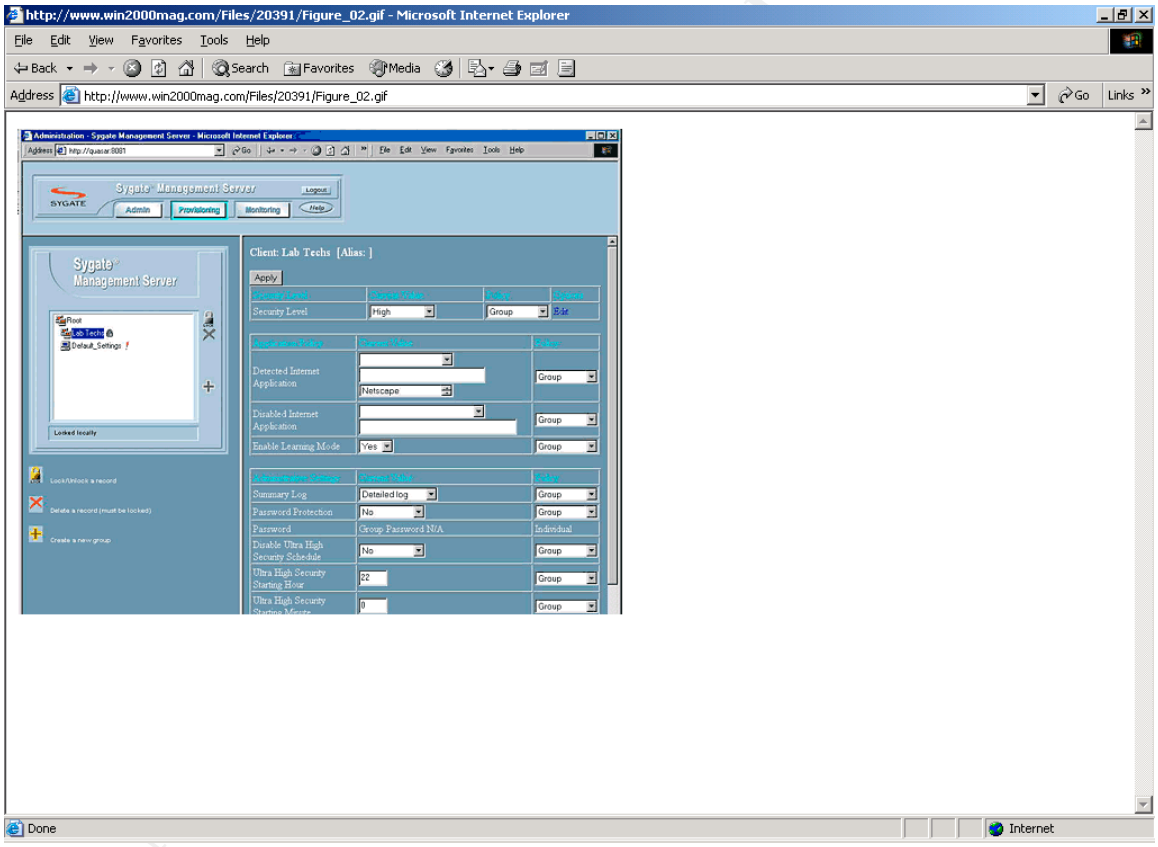

**(10)**

One of the advantages of PestPatrol's approach to deploying their enterprise security product is that it can be done without installing anything on client computers. The recommended starting point for deploying PestPatrol is the login script. PestPatrol and the login script must be installed on all the login servers (PDC's and BDC's). This script should load the real-time components of the software, minimize the effect on users at login by using the (/wait and /idle switches), require no user action if a threat is found, and then send all logs to a single email address if a pest if found.

A distinguishing feature of PestPatrol is that in addition to viruses, it focuses on non-viral malware such as Trojans, spyware, adware, hacker tools, zombies (Distributed Denial of Service Attacks). It will also work with existing security products and is compatible with all major anti-virus, firewall, and IDS installations.

## 4. "Sygate Secure Enterprise 3.5"

Sygate Secure enterprises 3.5 is an integrated product that helps companies control their network security by automating policy compliance. It also possesses the ability to enforce this policy on user endpoints. This Secure Enterprise suite is made up of a client-side security agent that runs on each remote host, a policy management server and enforcement servers at various network access points. The administration console is Java web-based and should be directed at the Sygate Management Server's host name and port (http://adminserver:port). The administrative console has three sections: Admin, Provisioning, and Monitoring.



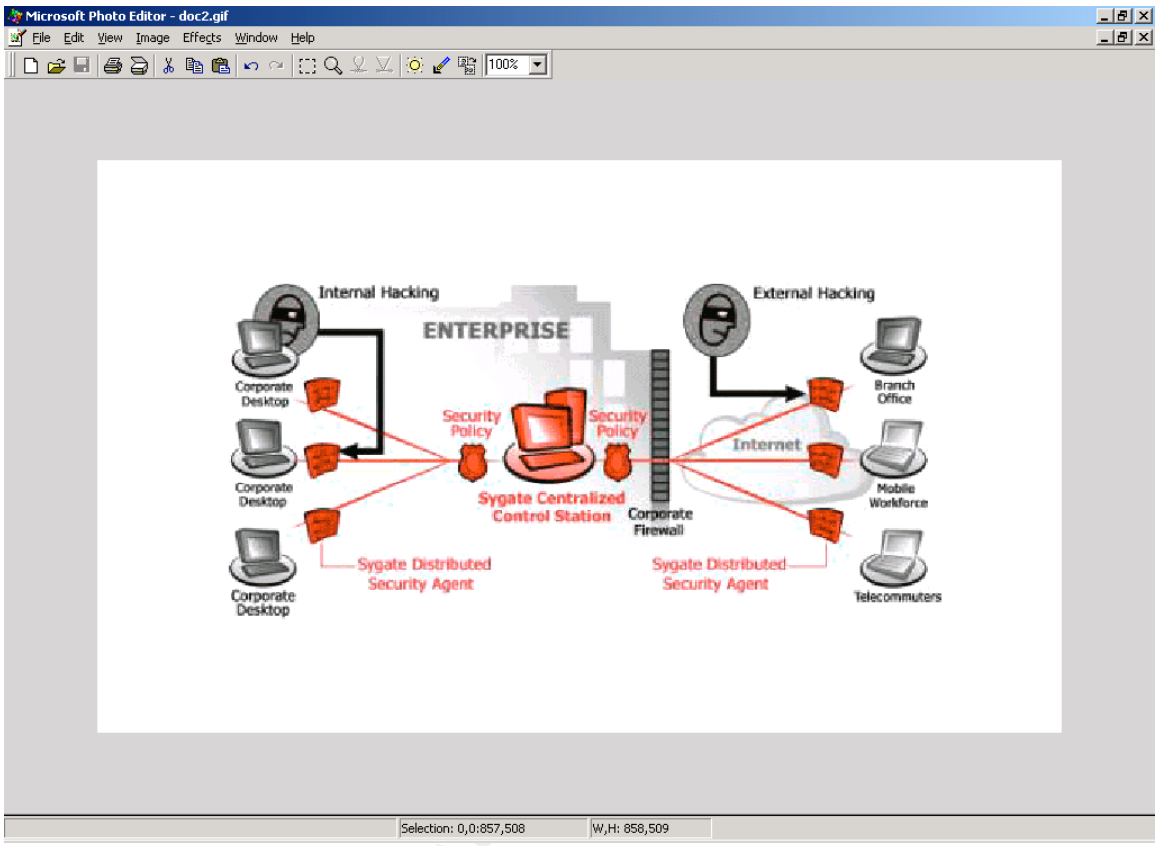

Shown above is the Sygate Management Server. **(11)**

Sygate Universal Enforcement ensures that endpoints that are non-compliant to established security policies will not be able to connect to the network, and will be quarantined until the remote host becomes compliant.

Automatic compliance is accomplished through security policy definition. The security policy can be setup and customized through **Sygate Management Server.** This policy enforces which executables should be running on the remote host. These files could include antivirus, host firewall, intrusion detection, along with the necessary patches and required registry values.

Non-compliant endpoints are quarantined. If the remote node is not compliant, the **Sygate Security Agent** can quarantine the agent while automatically starting corrective actions such as downloading and installing patches and turning on antivirus or the host firewall if the service is not running. The host can then be checked again for compliance.

Sygate Enforcers (optional) are network gateway devices that enforce remote host integrity at various network access points such as VPN's and dialup servers. The Enforcer challenges any host that requests entry to the network to see if the host is running a security agent and that the agent is compliant. If a Sygate Security Agent is not compliant, the Enforcer can block it from connecting to the network or can redirect it to a location to get the required updates.




Shown above is the Sygate Enterprise Security Solution. **(12)**

Although Sygate Secure Enterprise does not have its own antivirus component, it is compatible with all the major antivirus products. It does have a centrally managed personal firewall with logging, intrusion detection, and an enforced automatic host Policy compliance feature that makes it a good candidate for remote host security solutions.

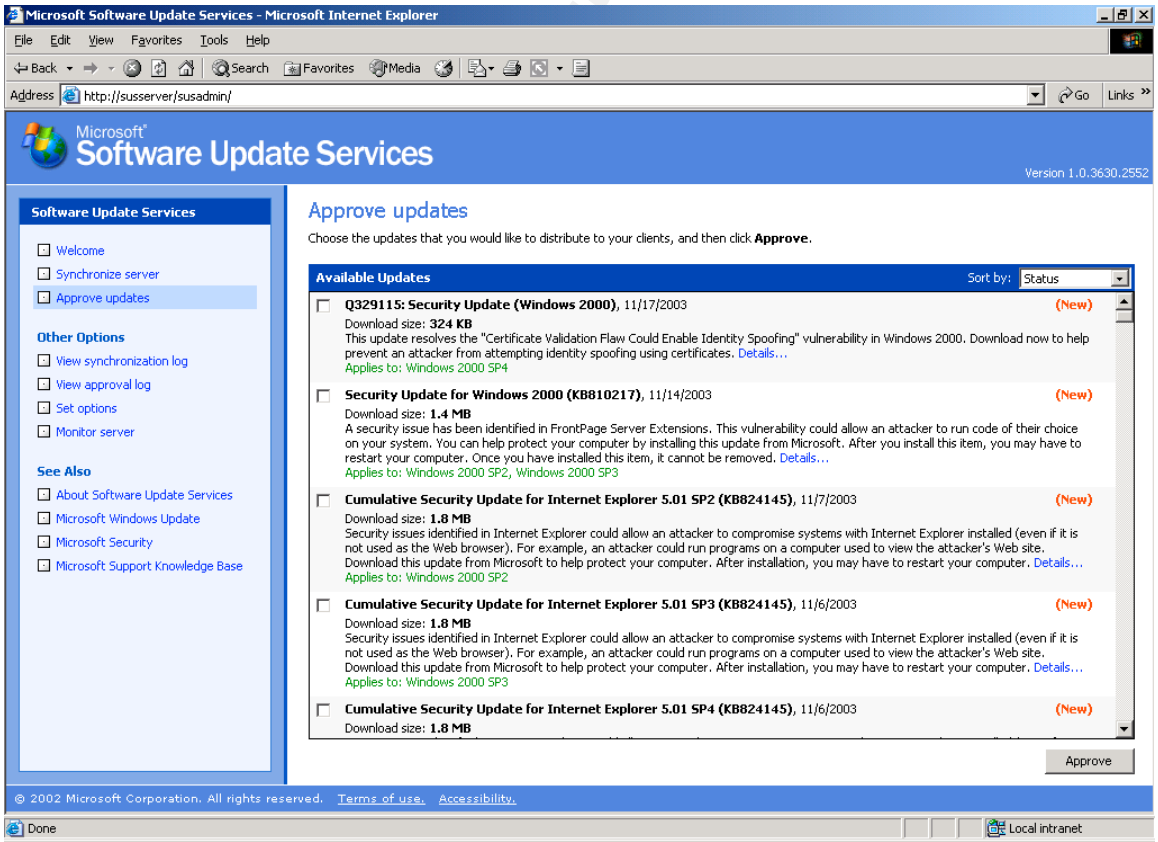
**Gratis vendor product that address remote host security:**

1. **The Microsoft Software Update Services (SUS)**

Microsoft Software Update Services is like having Microsoft Windows Update inside a corporate firewall. This allows for critical updates and security updates for Microsoft Windows 2000 Server, Windows 2000 Professional, Windows XP, and Windows Server™ 2003. SUS connects through a corporate firewall to the Windows Update site and allows IT administrators to import critical updates, security updates, and service packs. Unlike the Windows Update site, however, administrators maintain control over which items will be published internally to corporate servers and desktops**. (13)**

SUS consists of both client-side and server-side components to provide a basic solution to critical update management. The client is based on the Windows Automatic Updates technology for Windows XP. Automatic Updates is a proactive "pull" service that allows for automatic detection, download, and installation of required Windows updates such as critical operating system fixes and Windows security patches. It uses background Intelligent Transfer service (BITS), a bandwidth throttling technology to download updates (uses only idle bandwidth). When multiple updates are installed (chained installation), Automatic Updates installs them all together and this way the machine will only have to be rebooted once. Any logged-on users will be notified about pending reboots. Automatic Updates verifies that Microsoft has digitally signed the files before installing the downloaded updates.

The Software Update Services server side runs on Windows 2000 server. Internet Information Services (IIS) must be running on the server. The administrator can approve the updates before they are made available for download. A server running SUS can download packages from either the public Microsoft Windows Update servers or from another server running Software Update Services. Administration of SUS is web based. The administrator can use an HTTP connection or a secure SSL enabled HTTPS connection.




**(14)**

**Advantages:** Software Update Services is a patch management tool that will automatically download and install critical updates.

**Disadvantages:** Only supports Windows 2000 and later Windows versions. So if there is a mixed environment with several Windows 98 and/or Windows NT clients, these are not supported by SUS.

SUS is a free product from Microsoft to update critical security patches on a network's Windows 2000, Windows XP and Windows 2003 machines. While this product takes care of the patch question for remote hosts, the other remote security vulnerabilities (personal firewall, managed anti-virus software, security policy compliance), must be addressed by other products.

## Summary

This paper pointed out the importance of implementing some type of end-point security system with automated features. The network perimeter has been pushed further out with always-on broadband cable-modem and DSL Internet connections. It is no longer effective to rely only on a corporate firewall and routers to protect a network. Network security is an ongoing event. Companies, who adopt a host based security system in addition to their existing security infrastructure, would greatly improve their overall network security while lowering their total cost of network operations.

## References


1. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/msblaster.asp.

2. http://www3.ca.com/virusinfo/virus.aspx?ID=36376.

3. Ogren, Eric. “Host Intrusion Prevention is the Last Line of Defense for Networks: Yankee Group.” http://www.csoonline.com/analyst/report1265.html.

4. http://www.shavlik.com/pHFNetChkPro.aspx.

5. http://www.shavlik.com/pScanResults.aspx.

6. “Zone Labs Integrity – Enterprise Endpoint Security - Architectural Overview.http://download.zonelabs.com/bin/media/pdf/ZLInt45_archWP.pdf.

7. http://www.zonelabs.com/store/content/company/aboutUs/pressroom/graphicResourcesIntegrity.jsp.

8. http://www.zonelabs.com/store/content/company/aboutUs/pressroom/graphicResourcesIMSP.jsp.

9 “PestPatrol – Implementation Guide.” http://www.pestpatrol.com/productdocs/PPCEImplementationGuide.pdf

10. Screenshot of PestPatrol Corporate Edition console from John J. Dwyer’s personal workstation.

11. http://www.win2000mag.com/Files/20391/Figure_02.gif

12. “Guilty Until Proven Innocent: Next Generation Approach to Enterprise Security.” http://www.nwfusion.com/whitepapers/sygate/.

13. “Software Update Services Components and Features.” http://www.microsoft.com/windowsserversystem/sus/suscomponents.mspx

14. “Deploying Microsoft Software Update Services.” (January, 2003.) http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc.