

Thin Client Virus Vulnerability Analysis



| | |
|---|----|
| Virus vulnerabilities, encounters, and impact | 3 |
| Virus encounter vectors | 3 |
| Technology vulnerabilities | 4 |
| Impact of client computing vulnerabilities | 4 |
| HP Thin Client response to vulnerabilities | 5 |
| Diskette/removable media | 5 |
| E-mail/office applications | 6 |
| Web browser/Internet/Non-e-mail/peer-to-peer | 6 |
| Operating system | 6 |
| Instant messaging | 7 |
| Multimedia viewers | 7 |
| Thin client firewall | 8 |
| Sygate Security Agent | 8 |
| Recovery time | 8 |
| Locking down a thin client | 9 |
| Standard user rights | 9 |
| Least privileged user accounts | 9 |
| DisableCMD | 10 |
| Permission changes on the Desktop folder | 10 |
| Preventing file downloads from Internet Explorer | 10 |
| Preventing Disk-On-Key access | 10 |
| Hiding desktop items on the HP Compaq t57x0 Thin Client | 10 |
| Summary | 12 |
| For more information | 12 |

Enterprise computing networks require effective protection against computer viruses and other security issues. Security breaches can result in costly service calls, user downtime, and loss of business-critical data. When compared to the traditional unmanaged PC network model, the HP thin client computing model yields a less vulnerable segregated approach to computing with substantially better recovery time, while minimizing total cost of ownership (TCO).

According to an ICSA Labs virus analysis¹, the average downtime lost during an encounter is 23 person days. This downtime consists of data loss recovery and patching connected network servers and PCs.

With the HP thin client computing model, your vulnerability to virus attack on the thin client system is significantly less than a standard Windows PC. This means that thin client users will experience significantly less downtime due to security vulnerabilities than PC users. In addition, since no user data resides on a thin client, there is no risk of user data loss on the thin client. Finally, if a thin client's image is compromised or corrupted, recovery time is typically measured in minutes instead of hours.

Additionally, the HP thin client computing model utilizes PC blades and/or servers located in a data center. You can protect and monitor centrally-managed, data center resources more easily with antivirus and firewall tools. You can correct and recover compromised thin client resources faster and cheaper than distributed PC resources. The thin client model also allows you to segregate and centralize a user's data for easy backup and recovery, ensuring a higher level of service and security for your users at a lower TCO than distributed PC resources.

At HP, we realize security and TCO are important factors in enterprise computing. A Fall 2003 EDC survey showed more than 8 out of every 10 enterprises suffered a security breach as a result of malicious code. As a result, more than half of enterprises are increasing IT security budgets. HP believes the thin client computing model is an effective solution for the security-conscious enterprise.

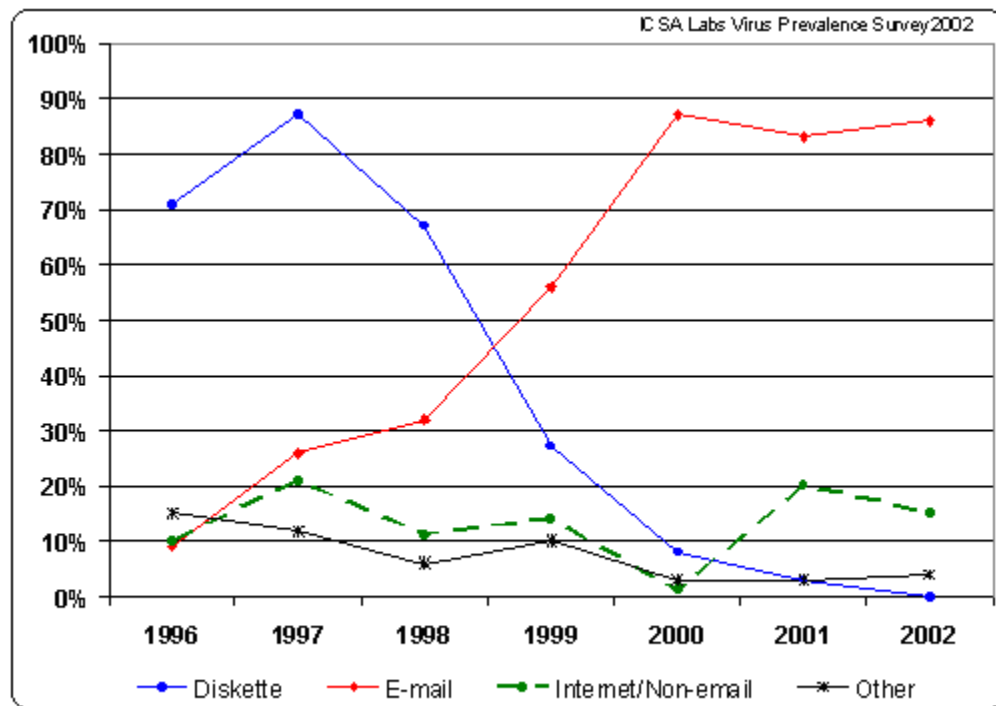
1. ICSA Labs 8th Annual Computer Virus Prevalence Survey

Virus vulnerabilities, encounters, and impact

The following graph depicts security vulnerabilities experienced by actual enterprise customers as surveyed by IC SA Labs for the years 1996 through 2002. The second graph contains the most vulnerable technologies as perceived by the enterprises surveyed in 2003 by EDC. The graphs illustrate a strong correlation between the actual occurrence of each vulnerability and its associated technology in an enterprise. For example, 86% of the encounters experienced in 2002 were e-mail related and according to EDC, 50% of the enterprises surveyed in 2003 perceived e-mail as their most vulnerable technology.

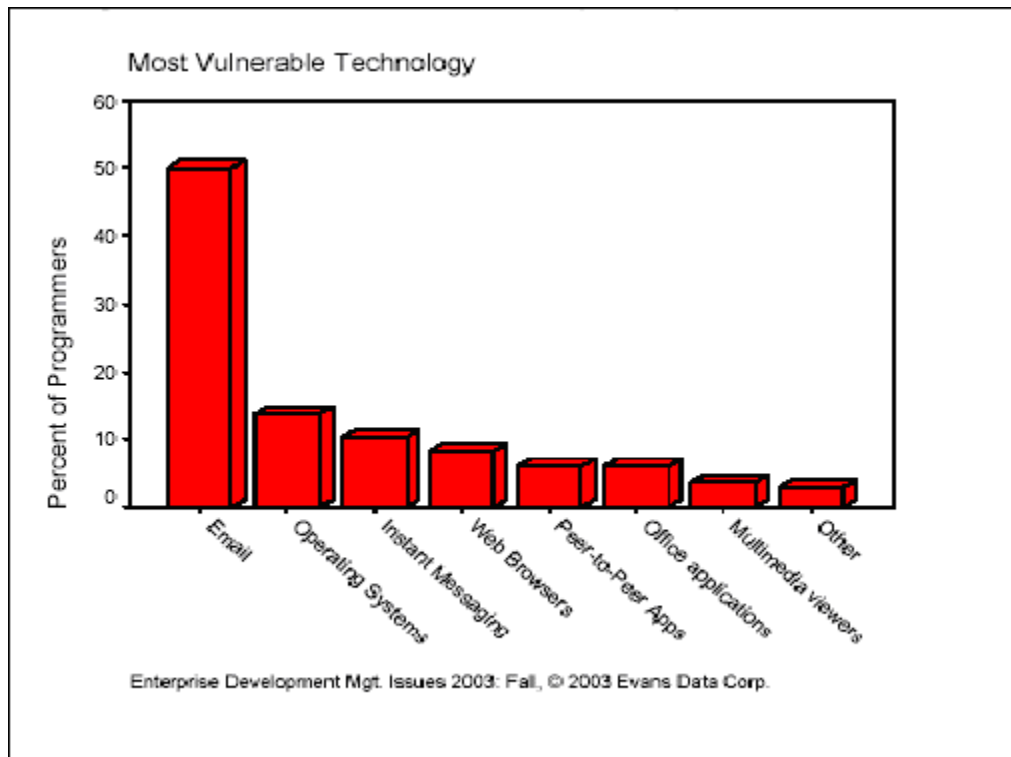
The third graph illustrates the impact of these vulnerabilities on the enterprises surveyed by IC SA in 2002.

Virus encounter vectors

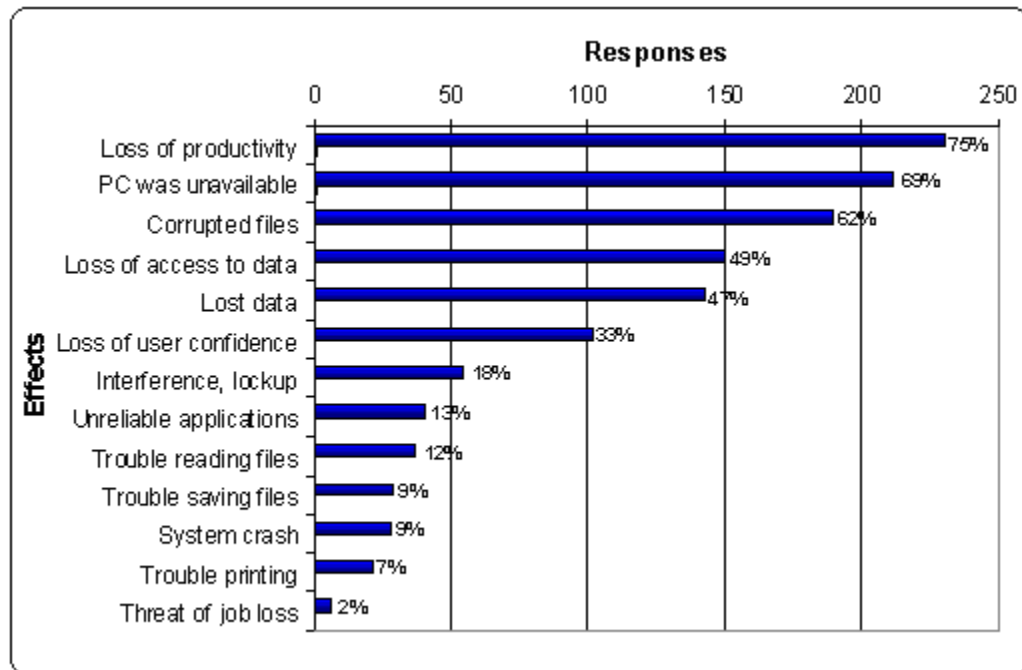


Note: "Other" in this graph represents unknown vectors and 3rd party/freeware software distribution.

Technology vulnerabilities



Impact of client computing vulnerabilities



HP Thin Client response to vulnerabilities

As the data in the previous section shows, the thin client computing model substantially reduces the likelihood that a thin client device will encounter a vulnerability as compared to a standard PC. The model also centralizes the enterprise's most vulnerable technologies in the data center, where you can effectively control and protect them from exposure at the user level.

The following table summarizes the previous data and shows that thin clients are substantially less susceptible to the virus vectors of attack and are exposed to fewer of the perceived vulnerable security holes than a standard PC. The following sections detail these areas as related to the thin client computing model.

| Technology | Personal Computers (PC) | | Thin Clients (TC) | |
|---------------------|--|---|--|---|
| | 2002 Encounter Vector Experienced ^a | 2003 Perceived Vulnerability ^b | 2002 Encounter Vector Experienced ^a | 2003 Perceived Vulnerability ^b |
| E-mail | 86% | 49.9% | 0% | 0% |
| Operating System | 0% | 13.5% | 0% | 13.5 |
| Instant Messaging | 0% | 10.1% | 0% ^c | 0% ^c |
| Web Browser | 4% | 8.1% | 0% ^c | 0% ^c |
| Peer-to-peer Apps | 11% | 6% | 0% | 0% |
| Office Applications | 0% | 6% | 0% | 0% |
| Multimedia Viewers | 0% | 3.6% | 0% ^c | 0% ^c |
| Other ^d | 4% | 2.9% | 0% | 0% |
| Total | 105% | 100% | 0% | 13.5% |

a. ICSA Labs Virus Prevalence Survey 2002

b. Enterprise Development Mgt. Issues 2003: Fall, © 2003 Evans Data Corp

c. This vulnerability is zero only if this component is not installed on the thin client device

d. Other in this table represents unknown vectors and 3rd party/freeware software distribution

Diskette/removable media

The intrusion of viruses from diskettes has declined significantly over the years and does not appear to be a significant vulnerability point. Still, a small percentage of virus encounters do occur through CD-ROMs and other removable media, typically when infected retail software is installed. Thin clients are predominantly deployed with no local removable drives such as CD-ROMs, diskettes, or hard drives.



E-mail/office applications

Using thin clients, users execute their e-mail and office productivity applications on centralized servers and/or blade PCs. These applications and their associated data execute only on the server/blade. The user interface for these applications is rendered locally on the thin client through Microsoft's Remote Desktop Protocol (RDP) or Citrix's® Independent Computing Architecture (ICA®) protocol. This means any virus or vulnerability introduced through your e-mail/office or other remote applications are remediated by the server/blade before affecting the thin client. Additionally, the administrator has total control over crucial applications and data on servers or blade PCs, and can readily manage and deploy virus and firewall protection to these centralized systems. While these back-end systems are at risk, applying patches or hot fixes to centralized computing resources is more cost effective and takes less time than it does for standalone PC systems. As a result, back-end servers are typically governed by security-conscious personnel.

Web browser/Internet/Non-e-mail/peer-to-peer

These attack vectors and technologies are a growing concern. The majority of infection occurs through infected/malicious code that is downloaded or shared through these technologies. Security holes in internet browsers are reported frequently. Browser-related intrusions are centered on JavaScript, Java Applets, Active X, unsigned or untrusted browser extensions, and so on. Also, some viruses and trojans propagate through instant messaging software.

The thin client model addresses these exposures in several ways. First, peer-to-peer applications and many Internet and non-e-mail Web services are typically not deployed on thin clients. The best thin client strategy is to deploy only what you need to achieve your business goals. Secondly, user initiated file downloads and sharing typically occur at the server/blade PC level and not on the thin client itself. The thin client typically does not provide the user with the space and access rights to support this. For example, on HP XPe thin clients, the Enhanced Write Filter (EWF) prevents permanent modifications (writes) to the contents of the system's flash. Finally, the Internet browser is an optional feature on select HP thin clients. Selecting models without it or optionally removing it ensures a more secure environment.

Operating system

Compared to a standard PC operating system, embedded operating systems are substantially smaller, providing less surface area to attack. Also, it is usually easier to configure an embedded operating system to have fewer services that can be exploited than it is for a standard operating system. Advantages differ based on operating system. Different operating systems are targeted at different rates and inherently have unique vulnerabilities. For example, Windows CE is substantially smaller and lighter than Windows XPe and is not targeted aggressively.

The following is a comparison of operating systems and their exposure on HP systems to the most exploited vulnerabilities of 2003 as listed by TruSecure®². As compared to a standard Windows PC, only two (MS03-026 and MS03-007) or around 22% of the nine most exploited vulnerabilities were relevant to the HP XPe thin client. The image includes patches for both.

² Wildtrends 2003: A Look at Virus Trends in 2003 and a Few Prediction for 2004; A TruSecure® Whitepaper

| Number of Viruses | Vulnerability Number | Exploited Vulnerability Name |
|-------------------|----------------------|---|
| 28 | MS01-020 | Incorrect MIME Header Can Cause IE to Execute e-mail Attachment |
| 16 | MS00-072 | Share Level Password |
| 6 | MS03-026 | Buffer Overrun In RPC Interface Could Allow Code Execution |
| 3 | MS99-032 | Scriptlet.typelib/eyedog |
| 2 | MS00-075 | Microsoft VM ActiveX Component |
| 1 | MS99-042 | IFRAME ExecCommand |
| 1 | MS00-043 | Malformed e-mail Header |
| 1 | MS00-046 | Cache Bypass |
| 1 | MS03-007 | Unchecked Buffer in Windows Component |

In addition to being a smaller target, the HP thin client XPe operating system contains an Enhanced Write Filter (EWF) that prevents damage to the local file system and its operating system files. The EWF protects the contents of the media by redirecting all the writes to a temporary virtual memory location. These writes are lost when the system is shutdown or restarted. It is also worth noting that none of these vulnerabilities were relevant to the HP CE-based and Linux-based thin clients. The Windows CE and Linux operating systems contain significantly different and less code than XPe. Lastly, the industry has yet to report a malicious virus on Windows CE.

Instant messaging

2003 saw a rise in viruses that infected devices using instant messenger (IM) clients. The proliferation of IM clients and greater acceptance of their use in corporate settings will continue to increase the attractiveness of this vulnerability for virus infections.³ Instant Messenger is an optional component on HP CE-based thin clients, whereas you can remove it from other operating system-based thin clients to ensure a more secure environment.

Multimedia viewers

This technology is a growing concern for security conscious network administrators. The majority of infections occur through infected/malicious code that is downloaded or shared on the Internet. Security holes in Internet Media Player have also been reported. Media Player-related intrusions are centered on requests and downloads of media files and skins. Additionally, a recent vulnerability in Media Player used malformed mp3 files to execute malicious code. HP has integrated Media Player into thin client images to support multimedia requirements; however, you can remove it from the image to ensure a more secure environment.

3. Wildtrends 2003: A Look at Virus Trends in 2003 and a Few Prediction for 2004; A TruSecure® Whitepaper

Thin client firewall

A key component to ensure a more secure computing environment is a firewall. HP integrates the Sygate Firewall into each Windows XPe image. HP also offers the Microsoft Windows Firewall as an optional add-on. If one of your systems on the network is compromised by malicious code, a firewall will help to prevent your thin client from infection. Additionally, a firewall helps to prevent external attacks from reaching your system, protecting against intruders infecting the thin client with malicious code.

The following sections show how to enable the Internet Connection Firewall feature to provide Internet security for your HP Compaq t57x0 thin client. This paper also discusses how to disable the Internet Connection Firewall feature, which may help in troubleshooting some applications that do not function as expected behind a firewall.

Sygate Security Agent

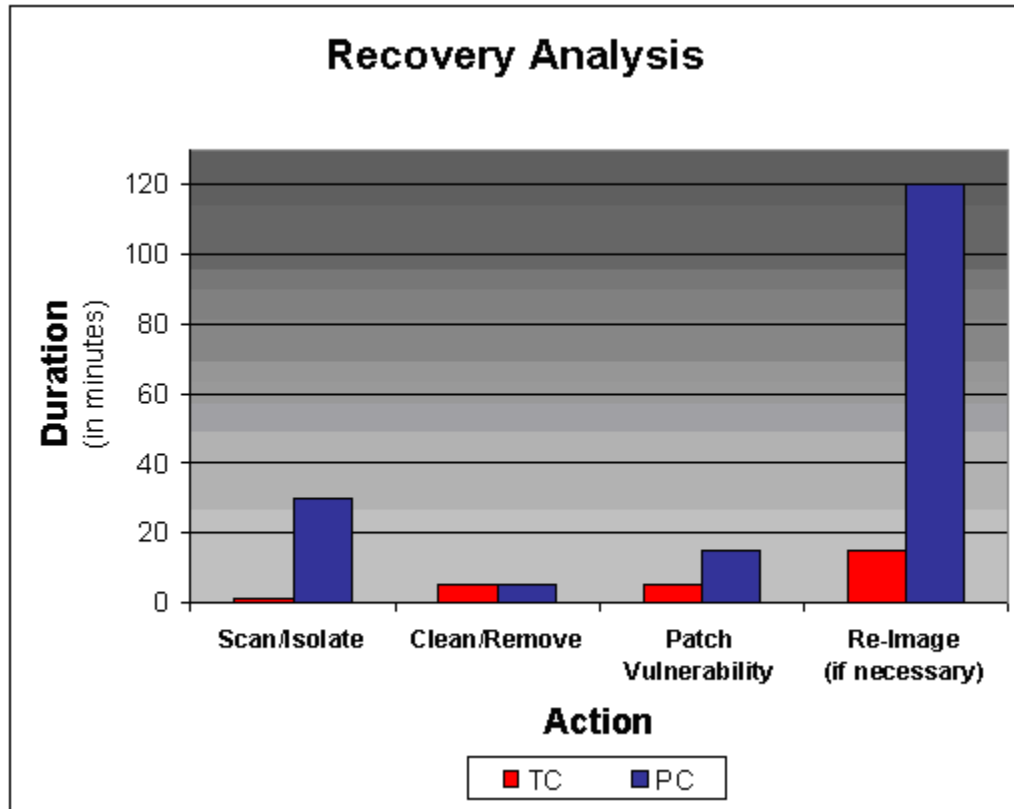
HP integrates the Sygate Security Agent into its thin clients. For more information about how this security agent can help you security your enterprise, see the white paper at <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00282639/c00282639.pdf>.

Recovery time

In the event of a virus attack or other security issue, the HP thin client computing model offers significantly shorter recovery time when contrasted with the traditional desktop model. If a thin client's image is compromised or corrupted, recovery time is typically measured in minutes instead of hours. Recovery usually involves a power cycle (1 minute), patch (5 minutes), or re-image (15 minutes) of the system. This is substantially less time than the typical two hours it takes to re-image a PC or the multiple hours that you can spend rebuilding and recovering a user's data and environment.

The following graph depicts the average recovery time of thin clients and desktop computers. In all categories, the HP thin client computing model meets or greatly exceeds the recovery speed performance of the traditional desktop computing model.





Locking down a thin client

Additional security is available for the HP Compaq t57x0 thin client series. Although the default User account on the t57x0 thin client is already somewhat locked down, the account does have administrative rights and can still allow activities such as downloading and executing programs to the desktop. You can further lock down a t57x0 by creating an account with non-privileged user rights (rather than administrative rights) and additionally applying more restrictive policies, such as preventing the user from downloading any files to the thin client. The following sections provide information and instructions for applying these restrictions.

Standard user rights

By default, a user account without administrative rights cannot modify drive C on a thin client. Furthermore, a user without administrative rights cannot commit changes using the Enhanced Write Filter.

Least privileged user accounts

A tool that provides added security is the use of a least privileged user account. For more information, see <http://www.microsoft.com/technet/security/secnews/articles/lpuseacc.mspx>.

DisableCMD

This command provides additional restrictions to a user account. The command prevents users from running the interactive command prompt, `cmd.exe`. This setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

NOTE: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.

Permission changes on the Desktop folder

An administrator can change the security permission on the Desktop folder so that it is read-only.

Preventing file downloads from Internet Explorer

An administrator can set permissions so that a user cannot download files from Internet Explorer. To restrict a user from downloading files from the Internet:

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.
3. Select the Security tab, and then click **Custom Level**.
4. Scroll down to **Downloads > File Downloads**.
5. Select **Disable** to prevent Internet downloads.

Preventing Disk-On-Key access

An administrator can disable Disk-On-Keys by performing the following steps:

1. Select **Start > Settings > Control Panel > System**.
2. Select the Hardware tab.
3. Click **Device Manager**.
4. Click **Disk Drives** to view all available drives.
5. Right-click on the device you wish to disable, and then select **Disable**.
6. To disable a USB device, select **Universal Serial Bus controllers**, then repeat steps 4 and 5.

NOTE: Future types of Disk-on-Keys may be developed that you cannot block using the above method.

7. To prevent users with administrative rights from enabling Disk-on-Keys, you can delete Device Manager after using it to disable the USB devices.

Hiding desktop items on the HP Compaq t57x0 Thin Client

Administrators can remove all or some items from a user's desktop using the `hide-stuff.reg` file. The `hide-stuff.reg` file will remove all icons from the start menu for the default user. It also removes the tray icon. This will allow the user to only double-click on the IE and/or remote desktop icons that are on the desktop. The `hide-stuff.reg` file contents are as follows:



REGEDIT4

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
```

```
"Start_ShowControlPanel"=dword:00000000
```

```
"Start_ShowMyComputer"=dword:00000000
```

```
"Start_ShowPrinters"=dword:00000000
```

```
"Start_MinMFU"=dword:00000000
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
```

```
"NoTrayItemsDisplay"=dword:00000001
```

```
"NoStartMenuMorePrograms"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage]
```

```
"Favorites"=hex:ff
```

You can modify the hide-stuff.reg file to include any icons. The following table is a list of definitions for each line of the file. To include a particular icon or item, delete the appropriate line.

| Code | Definition |
|--|---------------------------------------|
| "Start_ShowControlPanel"=dword:00000000 | Hide the control panel |
| "Start_ShowMyComputer"=dword:00000000 | Hide My Computer |
| "Start_ShowPrinters"=dword:00000000 | Hide Printers |
| "Start_MinMFU"=dword:00000000Programs | Hide Recently used |
| "NoTrayItemsDisplay"=dword:00000001 | Hide the Tray icons |
| "NoStartMenuMorePrograms"=dword:00000001 | Hide the More Programs Menus |
| "Favorites"=hex:ff | Hide Favorites from Internet Explorer |

After modifying the hide-stuff.reg file, perform the following steps:

1. Log onto the thin client as Administrator.
2. Copy the attached file into c:\Documents and Settings\User\Desktop\.
3. Log off, and then log on as User.
4. Double-click the hide-stuff.reg file on the desktop.
5. Click **Yes** in the warning dialog box.
6. Click **OK**, and then log off.



7. Log on as Administrator.
8. Delete c:\Documents and Settings\User\Desktop\hide-stuff.reg.
9. Log on as User.
10. Click **Start**. Verify that the icons no longer display.
11. Make sure that the hide-stuff.reg is removed from the desktop, and then log off.
12. Log on as Administrator.
13. From Control Panel, start the EWF Manager.
14. Click **Commit data to volume**, and then reboot.

Summary

The HP thin client computing model provides significantly better virus protection than its PC counterpart. This protection is achieved by:

- Centralizing an enterprise's computer resources in the more secure and controlled data center.
- Using centralized virus protection and firewall tools to protect these resources.
- Segregating the user's data for enhanced security, backup, and quick recovery.
- Deploying HP thin clients for simple, secure, reliable, and efficient access to these centralized resources.
- Using HP centralized management tools to manage and patch at all levels of the enterprise.

For more information

For more information about HP Compaq t5000 thin clients, see:

http://h18004.www1.hp.com/products/thinclients/index_t5000.html

© 2006 Hewlett-Packard Development Company, L.P. The information in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation in the U.S. and other countries.
367974-003, 1/2006



867.1191
sales@nexustech.com.ph
www.nexustech.com.ph

