Security with Windows® XPe

The Wyse® implementation of the thin client operating system is as secure, or better, than PCs and other thin client devices. Since disk drives are not standard in thin clients, data is almost never lost, stolen, or corrupted by mechanical failure, virus, or malicious attacks. Therefore, thin clients are a key component of a secure computing environment.

Base Operating System
All currently shipping Wyse XP Embedded (XPe) thin clients come with Microsoft XP Windows Embedded Service Pack 2 which provides the same broad range of security changes to Windows XP Embedded that Windows XP Professional SP2 includes. Also, the Windows Firewall is standard on Windows XPe increasing the security of your thin clients.

Units with older code are, in most cases, fully upgradeable to the latest Windows XPe image release from Wyse (this may not be the case for all older units as new images are not created for unsupported platforms). Going forward, Wyse units remain upgradeable via re-imaging to newer image versions when released.

Vulnerability Protection
Most vulnerabilities, virus and malware are transferred by Internet browsers, email attachments, or by opening infected files in the local storage devices. Microsoft Windows XPe SP2 provides pop-up blocker and the capability to block both unknown and unsigned ActiveX controls. Also, in the thin computing environment, Wyse thin clients rely on the server-based email clients, when malicious mails or attachments are opened, they do not traverse or propagate to other thin client devices.

When local storage devices are attached, they could introduce security vulnerabilities for intrusion. You can even equip Wyse thin clients with any number of anti-virus solutions, although this is often overkill, and not used extensively by Wyse customers.

Write-Protection
The Enhanced Write Filter (EWF) feature of Windows XPe makes it possible for you to write-protect your run-time images. All Windows XPe units from Wyse come with either Wyse's (SP1 units and earlier) or Microsoft's Enhanced Write Filter.

When enabled, this feature prevents permanent writes to the local media which means that your Wyse unit won't suffer from a permanent virus. This does not prevent viruses which install to RAM and propagate without requiring a reboot, but it does mean that a simple reboot of the unit will clear any such virus and return the unit to its clean state.

Firewall Protection
All Wyse XPe SP2 units ship with Microsoft's Windows Firewall as part of the base OS. Wyse does not enable this by default and so the activation of this feature is at the discretion of the customer. This solution, and others like it, has proven effective against the spread of viruses but can reduce versatility at the client level. It will require an increased level of testing to ensure that all local functions on the client perform as expected and required before any deployment.

Wyse Security Policy Statement
Wyse Technology Inc., is dedicated to provide the latest security updates from Microsoft and to help our customers comply with mandates such as Sarbanes Oxley, HIPAA, and others.

Microsoft's monthly security updates remain the best proactive solution for anti-virus available for Windows XPe devices. It is Wyse's policy to convert and publicly post in the Wyse Device Manager format all necessary Security Updates and Patches within 10 business days of the XPe* releases from Microsoft. Some Microsoft Security Patches might be resolved faster depending on the severity and customer impact.

It is recommended that customers apply these updates when available. Fully patched units are nearly invulnerable to viruses and attacks. It is Wyse's stance that this is the single most important thing that can be done to protect units from attacks and represents a significantly more secure and predictable situation than any form of anti-virus or firewall on the local client.

* Note that XPe patches and security updates are normally released by Microsoft several days after the XP releases.