

Windows Vista (DARC)

Matthew Cook

<http://escarpment.net/>

<http://darc-tech.org.uk/>

Introduction to Vista

- Five years worth of development
- Complex and big product
- Many versions
- Lots of under the hood changes
- 32bit or 64bit

- Time to upgrade?

What is wrong with XP

- Mid 2001 Windows XP and Mac OS X
- Vista – Longhorn case of mistaken identity?
- RSS, Gadgets, Browsers, Search etc
- XP 99.9% Compatible
- Known knowledge base
- If it does everything I want?

How many versions?

- Microsoft Windows Vista:
 - Starter
 - Home Basic O£56 U£80 F£164
 - Upgrade £82 Basic -> Premium
 - Home Premium O£73 U£119 F£180
 - Business O£87 U£143 F£203
 - Upgrade £112 Business -> Ultimate
 - Ultimate O£120 U£180 F£290
 - Enterprise
 - N Series

User Interface

	Home Basic	Home Premium	Business	Enterprise	Ultimate
Windows Vista Basic UI	Yes	Yes	Yes	Yes	Yes
Windows Aero UI ("Glass")		Yes	Yes	Yes	Yes
Windows Flip	Yes	Yes	Yes	Yes	Yes
Windows Flip 3D		Yes	Yes	Yes	Yes
Live Taskbar Thumbnails		Yes	Yes	Yes	Yes
Instant search	Yes	Yes	Yes	Yes	Yes
Live content organization in Explorer windows	Yes	Yes	Yes	Yes	Yes ₅

What are you missing? Home Basic or Premium

- Basic
 - Scheduled Backup
 - Shadow Copy
 - System Image
 - EFS
 - Bitlocker
 - Premium Games
 - Media Centre
 - Projector/Presentation
 - Join Domain
 - Offline Files
 - IIS Web Server
 - Tablet PC
 - Touch Screen
 - Windows Sideshow
 - Fax and Scan
- Premium
 - Shadow Copy
 - System Image
 - EFS
 - Bitlocker
 - Join Domain
 - Offline Files
 - IIS Web Server

Installing Windows Vista

- Where has DOS gone?
- Setup DVD
- Multiple images
- 25mins
- Single expanded image to copy
- Slipstreaming – Updates folder
- Clean or Full Install

Specification

- Vista Capable
 - 800Mhz, 512Mb, Direct X 9
- Vista Premium
 - 1Ghz, 1Gb, Direct X 9 (128Mb), 40Gb, DVD
- Vista Realistic
 - 2Ghz, 2Gb, 256Mb Graphics Card
- Vista upgrade advisory

Parallel Running

- Dual Boot
 - Be careful
 - Backup
 - Norton/Symantec GoBack
 - Linux
- VMware
 - Later V5 or V6
- Buy a new PC!

First Appearances

- Slick GUI
 - Like OS X
- Less MS DOS
- Abstraction of services
- A lot has changed
- Aero Glass
- New icons
- New sounds
- 6 sec less on boot time

New Features

- Desktop Search
- Start Orb
- Start Menu
- Ready Drive Support
- Ready Boost Support
- Windows Experience Index
- Windows Super Fetch
- Real Processors, Cores and RAM

New Features 2

- Reliability Monitor
- Backup and Recovery
 - Automated System Restore (ASR)
 - Windows Complete PC Backup
 - .vhd files NOT in Home Basic Premium
 - Backup and Restore Centre
 - System Restore
- Shadow Copy – Previous Versions
- EFS

New Features 3

- Windows Calendar
- Windows Contacts
- Windows Sidebar
- Games Explorer
- Windows Photo Gallery
- Windows Media Player 11
- Windows Movie Maker
- Windows DVD Maker

Under the hood

- Enhanced Buffer Overflow Protection
 - NX bit in hardware
 - Address Space Layout Randomisation
- Services
 - More services by default
 - Restricted Services
 - Per service ACLs
- Signed drivers
- Kernel Patch Protection (x64)

Logon

- GINA
- User Account Control
 - Standard User or Administrator
 - Administrator Approval Mode
 - File system and registry virtualisation

Internet Explorer 7

- New architecture
- Phishing Filter
- SSL Certificate Warning
- Protected mode (in Vista)
 - Default, except in trusted zone
 - Uses new layering technology
 - User Account Control
 - Integrity of Applications
 - Process Privilege protections
 - Restrict Access
- Fix My Settings

Microsoft Security Centre

- Firewall
 - Monitors egress traffic
 - Location aware improvements
- Windows Defender
 - Software explorer
- Monitoring Improvements
 - Anti Virus
 - Anti Spyware
 - Firewall
 - Microsoft Update
 - Internet Explorer Settings
 - User Account Control

Filing System Protection

- BitLocker Drive Protection
 - Accidental data disposal
 - TPM
 - Encryption keys and RIPA Part 3
- Enhancements to traditional EFS
- Connection of USB devices
 - USB Sticks
 - USB hard discs
 - iPods etc

Networking Changes

- Network Access Protection (NAP)
 - Posture checking
 - Isolation
- Network Awareness
 - Connectivity
 - Connections
 - Location
- Network diagnostics framework
- Wireless improvements
- TCP Offloading support
- SMB 2.0

Network Posture

Windows XP IPv4

135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
1025/tcp	open	taskscheduler

Windows Vista IPv4/6

135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
5357/tcp	open	wininit.exe
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	lsass.exe
49157/tcp	open	services.exe

IPv6

- Redesigned IPv6 network stack
- Enabled by default
- Conversations on local subnet
- AAAA DNS Lookups
- IPSec support
- Teredo NAT Tunnelling

Image X

- WAIK CDImage Download WinPE2
- `ImageX /compress /capture <drive> <path>`
- `/compress <none|fast|high>`
- `ImageX /apply <path> 1 <drive>`
- .wim File based, not sector based
- Multiple images per .wim file

CLI

- Command Line
 - Its still there, cmd.exe
 - Auto completion
 - History

Resources

- Administering Windows Vista Security
The Big Surprises
 - Mark Minasi
 - ISBN 0-470-10832-0
- Microsoft Windows Vista Resource Kit
 - Microsoft
 - ISBN 0-735-62283-3

Conclusions

- Many features not included with Home
- Media Protection DRM
- Memory hungry
- Speech recognition

Questions and Answers

<http://escarpment.net/>

<http://darc-comp.org.uk/>