Windows 7 Security

Jorge Orchilles

Terremark Worldwide

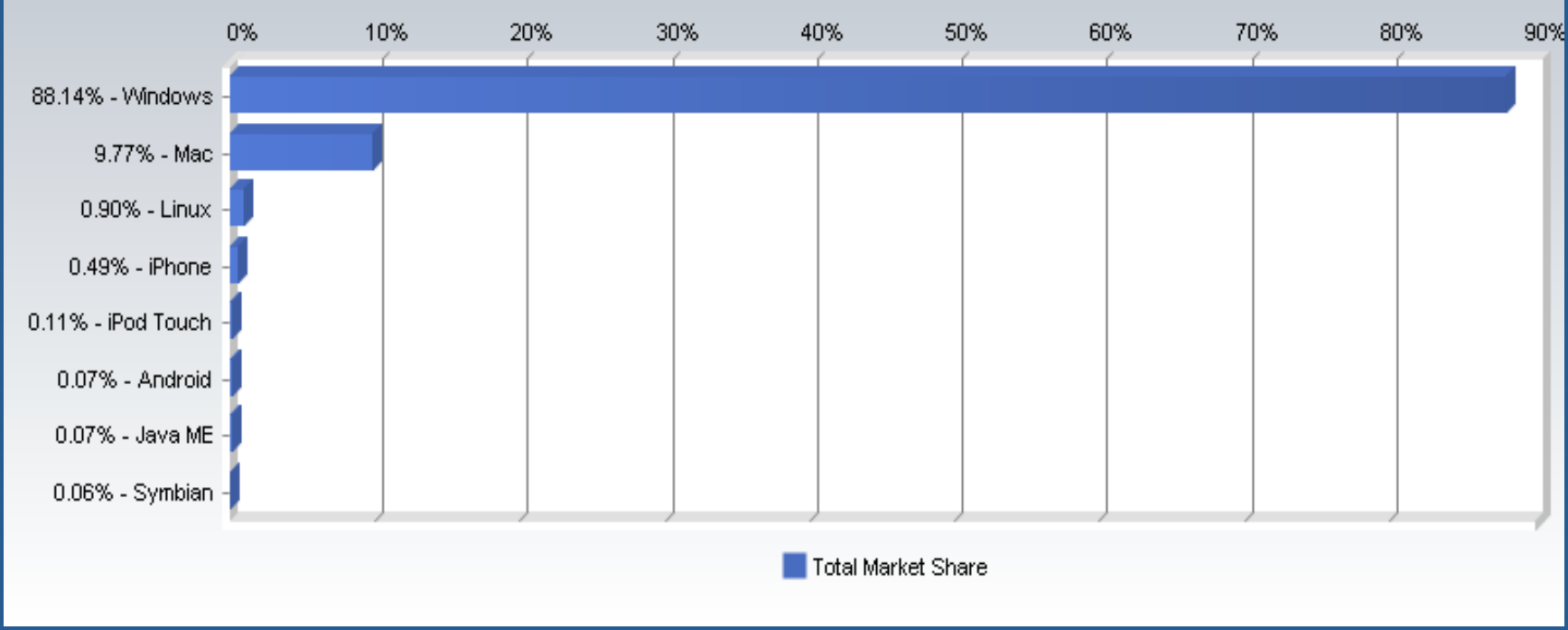
About Me

- IT Consultant over 7 years ago
- Security Analyst at Terremark
- Master's of Science in Management Information Systems @ FIU
- Author of Microsoft Windows 7 Administrator's Reference, Syngress Publishing
- Few certs: CCDA, CSSDS, MCTS, MCP, Security+

Audience Survey

- XP Users?
- Vista Users?
- Windows 7 Users?
- Mac OS X?
- Linux/Unix?

Reality



March 2009 Survey - ComputerWorld

- 88% Windows
- 10% Mac
- 1% Linux

Reality

- Up to 94% of corporations skipped Windows Vista
- New PC users had a choice to “downgrade” to XP
- New OEM PCs will include Windows 7 and no choice for Windows Vista or XP for that matter.
- All enterprise systems will be required to upgrade to either Vista or Windows 7 soon! Microsoft is threatening cut off dates already.
- Windows XP is 8 years old!

Windows Vista

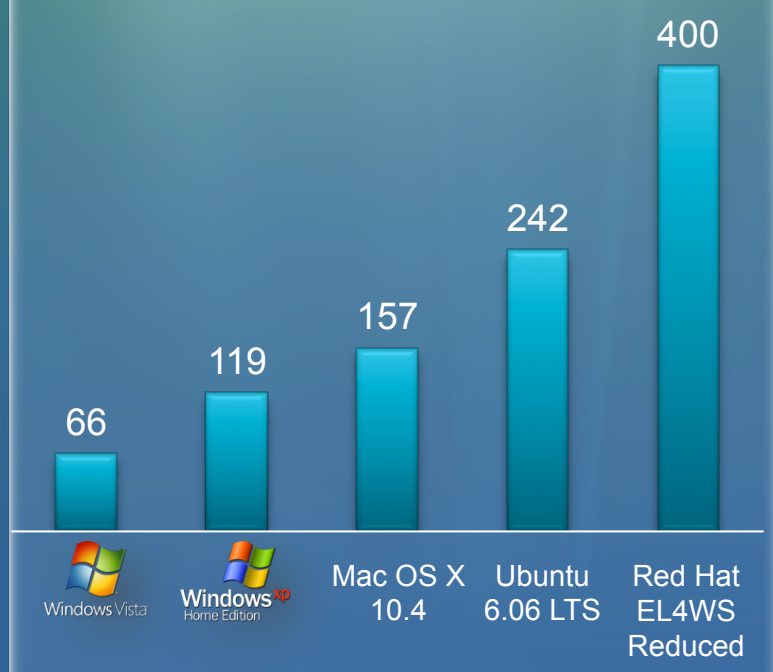
FAIL?

Why?

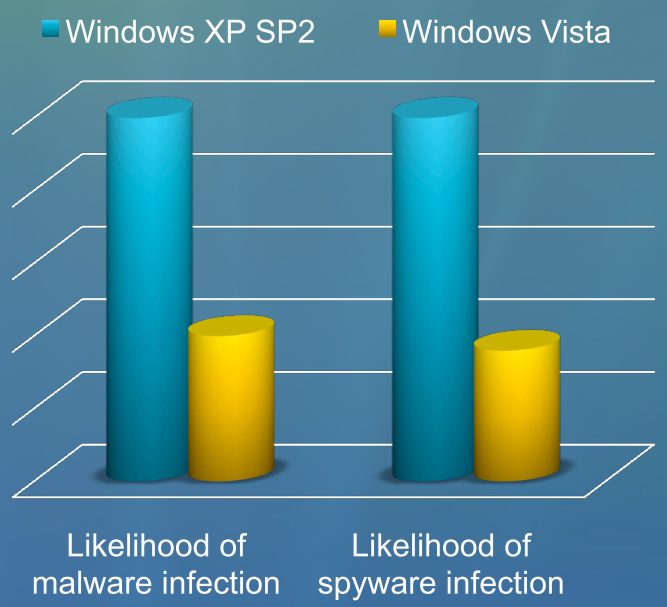
- Bad Press
- Horrible release

Windows Vista - Security Fail?
Not so much

Fewer High Security Vulnerabilities in Year 1



60% Fewer Malware Infections Than Windows XP SP2



Windows Vista - Security Features

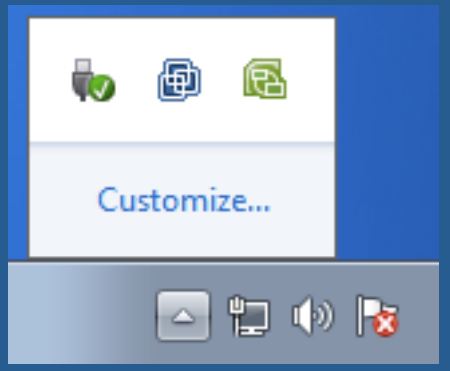
- Security Development Lifecycle
- Windows Service Hardening
- Windows Defender
- Internet Explorer 7 w/Phishing Filter
- NG TCP/IP –IPv6, IPSec., WFP
- Vista Firewall – inbound and outbound
- Network Access Protection
- User Account Control – consent and credential prompting
- Code Integrity – all OS DLLS and exec digitally signed
- BitLocker, Encrypted File Systems, & Trusted Platform Module

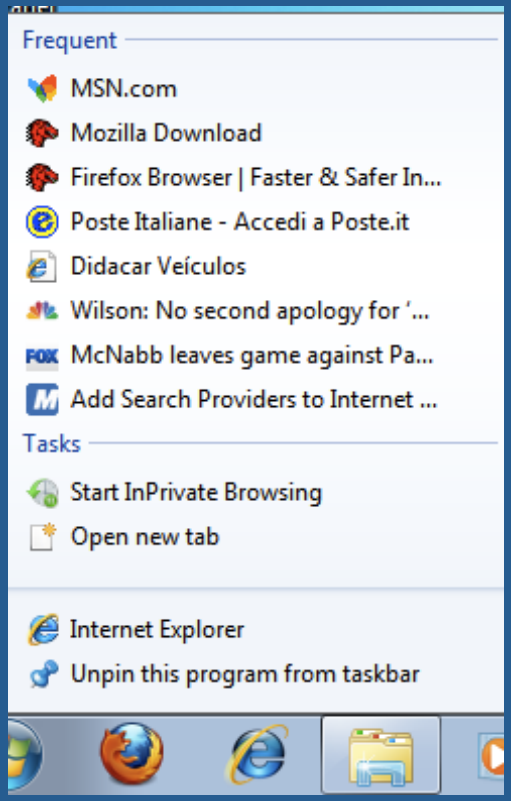
Introduction to Windows 7

- Incremental update to Windows Vista
- Uses the same technologies already in place with Vista
- Simpler user interface and enhancements to performance
- Extensive UAT via public Beta and RC

New Desktop Features

- User Interface
  - Taskbar – Notifications
  - Aero Peak and Aero Snap
  - Jump Lists
- Desktop Search
- Driver and Device Support
- HomeGroup
- Windows Media Player/Center





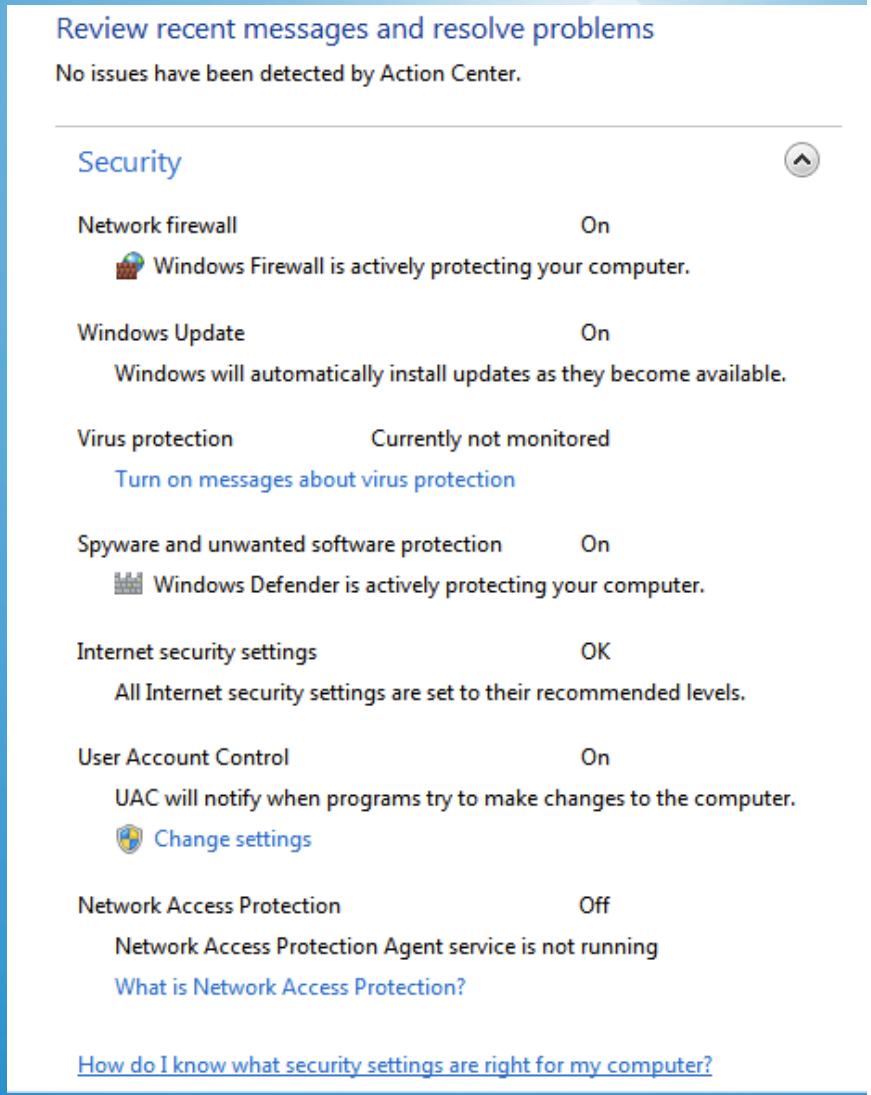
Security Features

- Action Center
- Better UAC
- Better BitLocker
- BitLocker ToGo
- Biometric security
- Internet Explorer 8
- AppLocker
- DirectAccess
- PowerShell v2

Action Center - Security

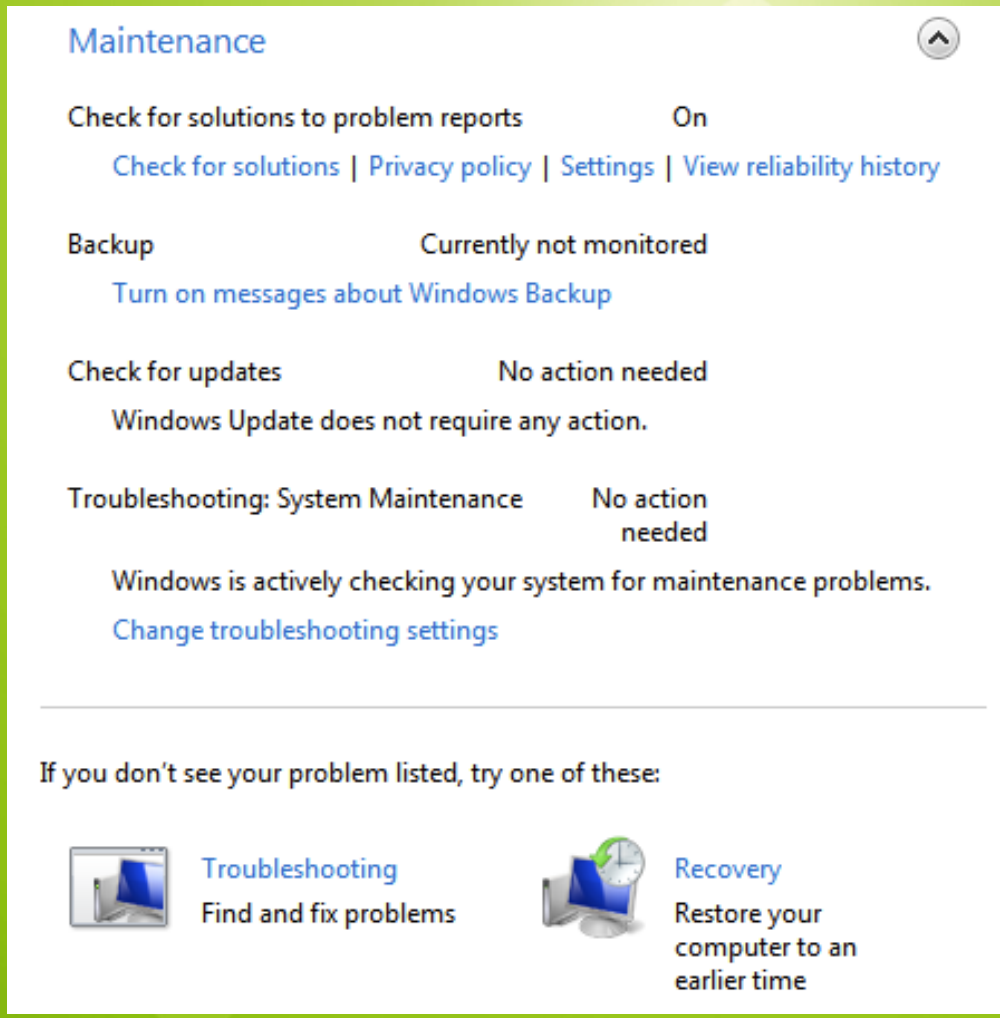
Replaces Security Center

- Firewall
- Windows Update
- Virus Protection
- Spyware / other malware
- Internet Security Settings
- User Account Control
- Network Access Protection



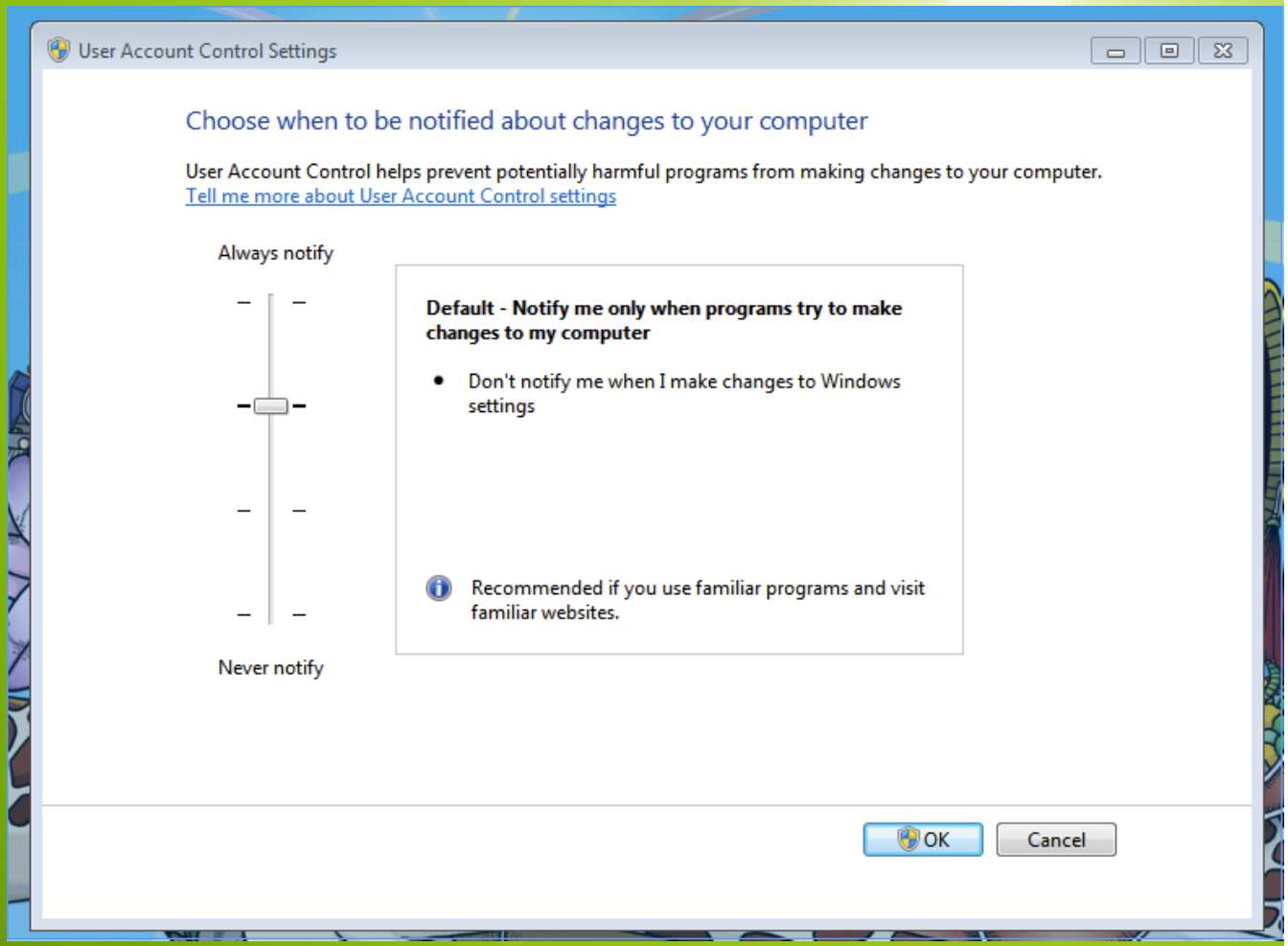
Action Center - Maintenance

- Check for solutions to problems
- Backup
- Check for updates
- Troubleshooting
- Recovery



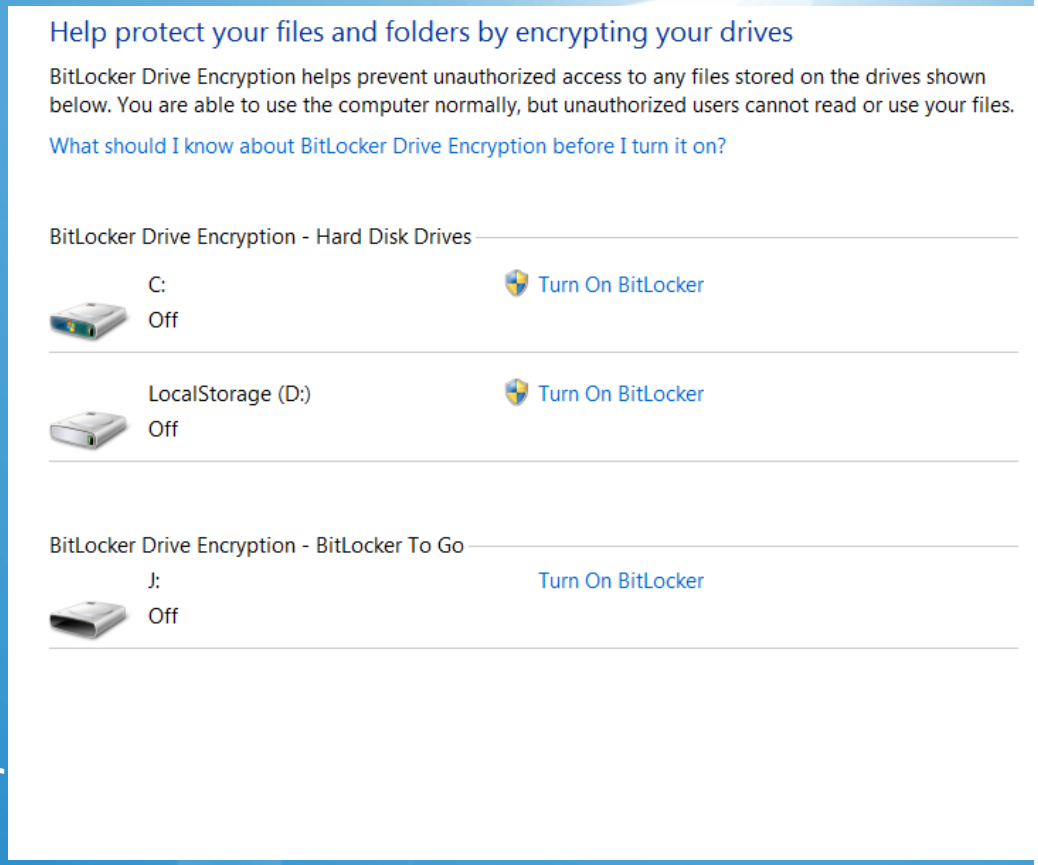
User Account Control

- Less nagging
- GUI for customizing
- Helpful?



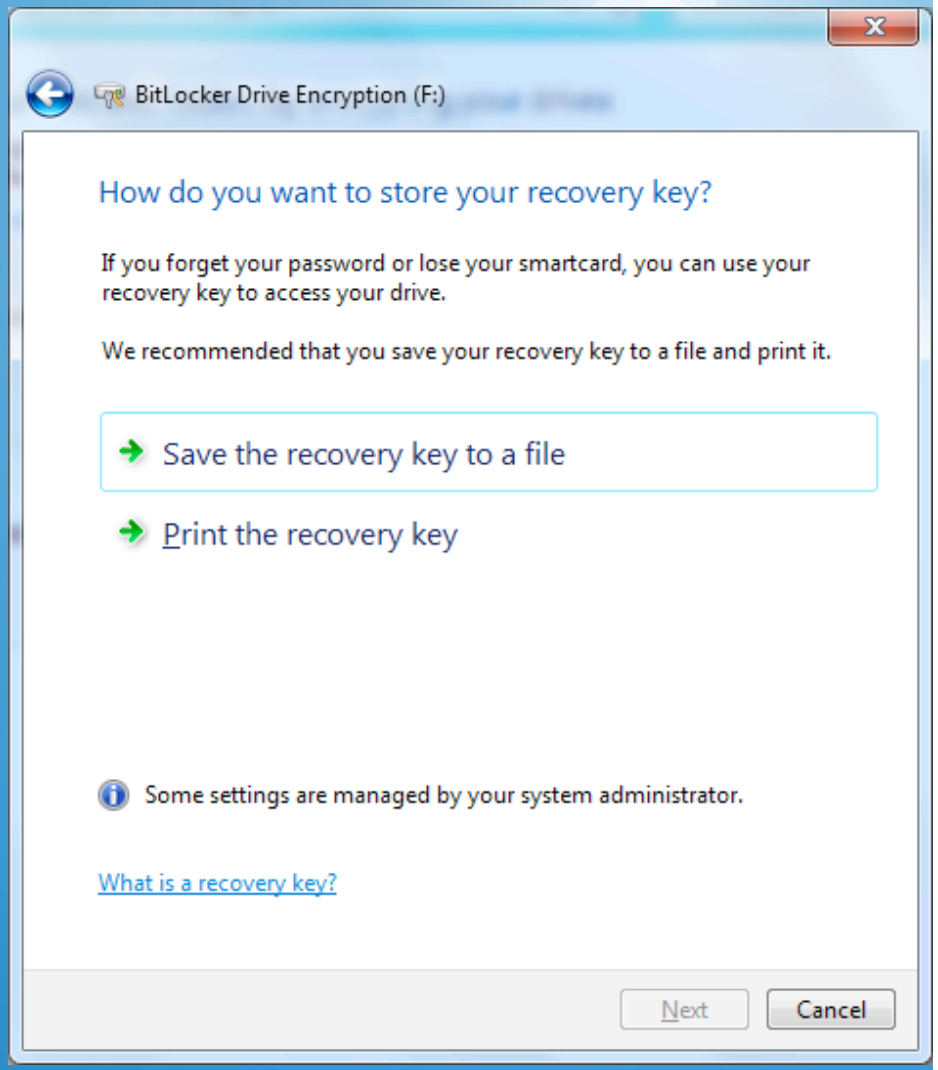
BitLocker

- Introduced in Windows Vista
- Encrypts the system volume, including the page file and hibernation files
- No need for partitioning!
- Whole drive/volume encryption
  - Trusted Platform Management (TPM) chip or pin/USB key



BitLocker – Recovery Key

- *All* Bitlocker deployments require a copy of the recovery password to be stored somewhere
- Out of the box, your users must save their own recovery password
  - This probably isn't the best idea…

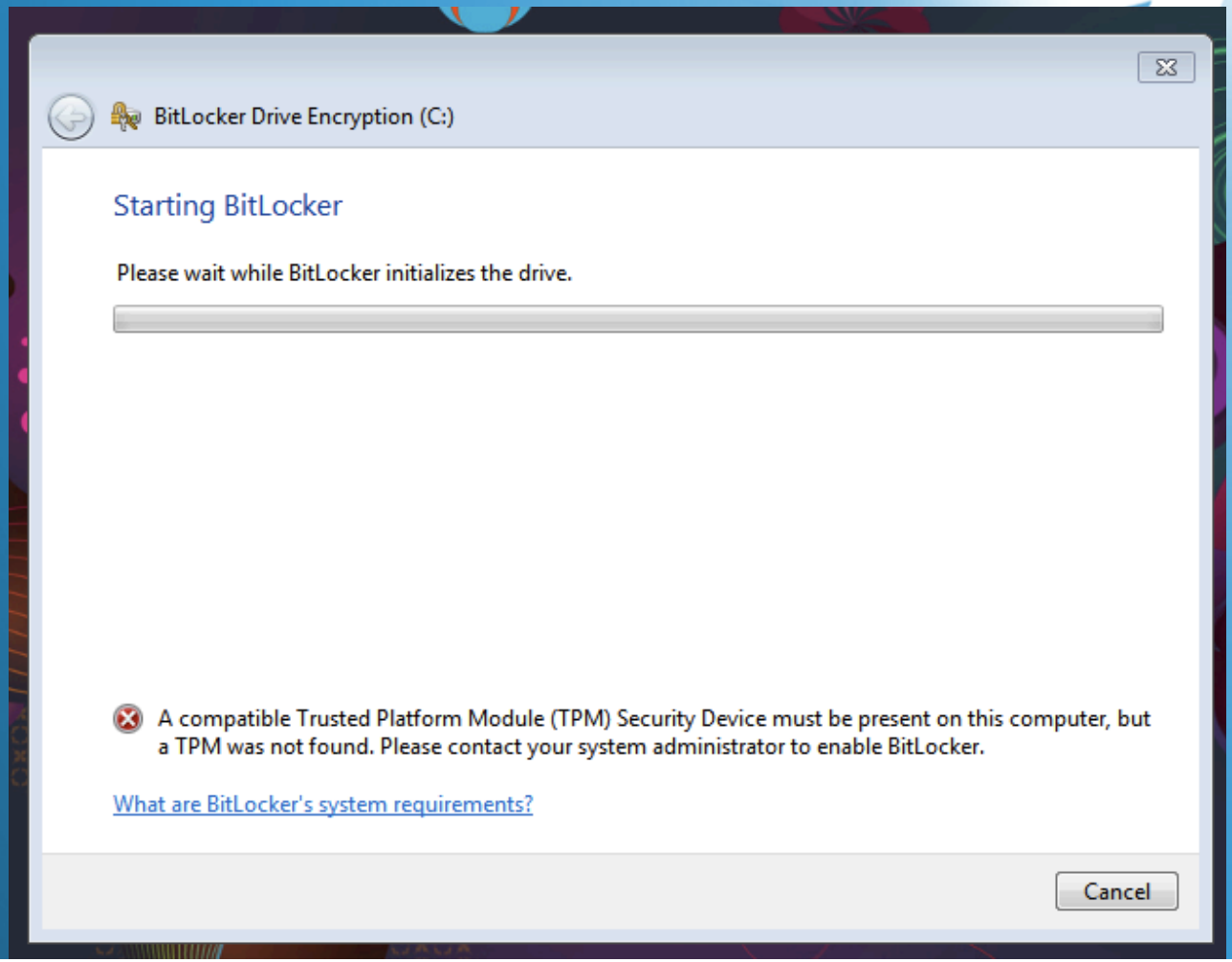


BitLocker - Issues

- High security environments can require a pin # or USB key before the system will boot
  - Remote systems or servers in datacenter - BEWARE
- BitLocker is *not* a replacement for EFS
  - BitLocker protects the whole drive at boot
  - No protection from user A seeing user B's files post boot
  - EFS solves this problem

BitLocker - Issues

- Trusted Platform Module required



BitLocker – Corporate Environment

- Requires Windows Server 2003 SP1 or newer domain controllers
- Group Policy – Require Encryption!
- Universal Recovery Key: Data Recovery Agent
- What about deleted/disabled computer accounts?
  - Sales guy who's always on the road
  - High-powered exec who goes on a 3-month sabbatical

BitLocker To Go

- Encrypt Removable Media
- Lost USB drive with corporate information?

Survey: 40% Of Workers Have Lost A USB Stick

Nearly two-thirds also have left a drive unprotected in a PC, BlockMaster reports

Updated An Ealing council employee infected the UK local authority's IT systems with the Conficker-D worm after he plugged an infected USB into a work computer, causing tens of thousands of pounds in damages in the process.

http://bit.ly/iJv4v
http://bit.ly/1zFl3

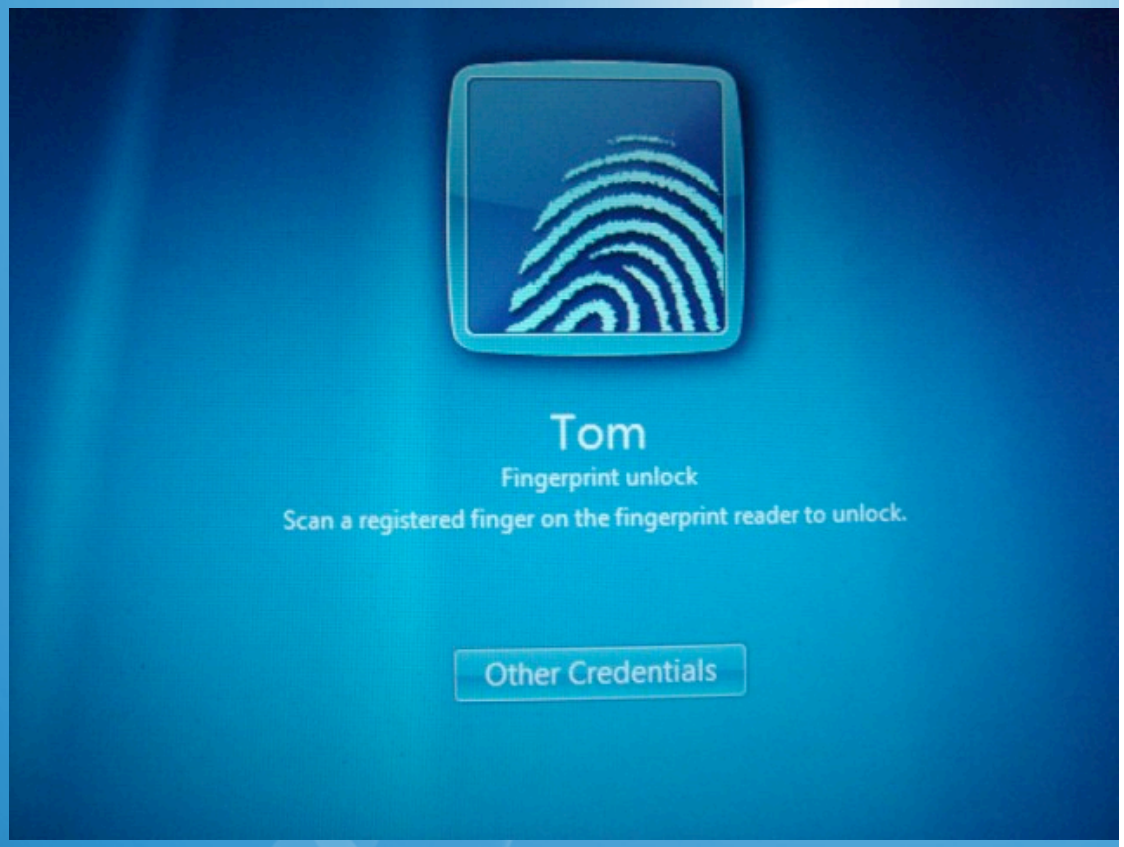
Windows 7

BitLocker To Go - Issues

- Does not work with other OS
  - FAIL
- On Vista and XP you can view content but not edit
  - FAIL
- Password based
  - Recovery file?
  - Brute force?

Biometric Security

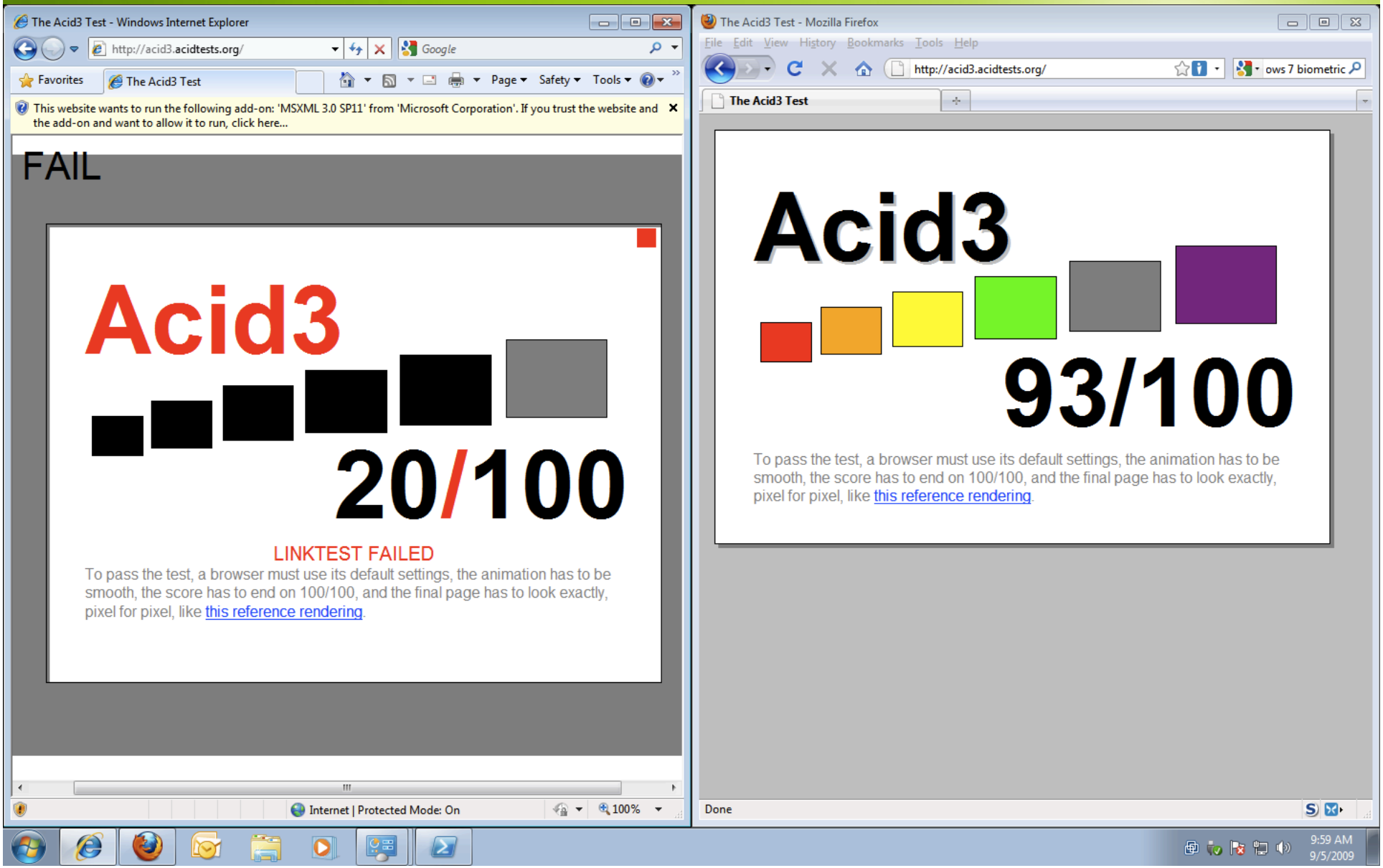
- Options with most new laptops
- Had to use OEM software
- HP Biometric Security – FAIL
- Can login Local or Domain



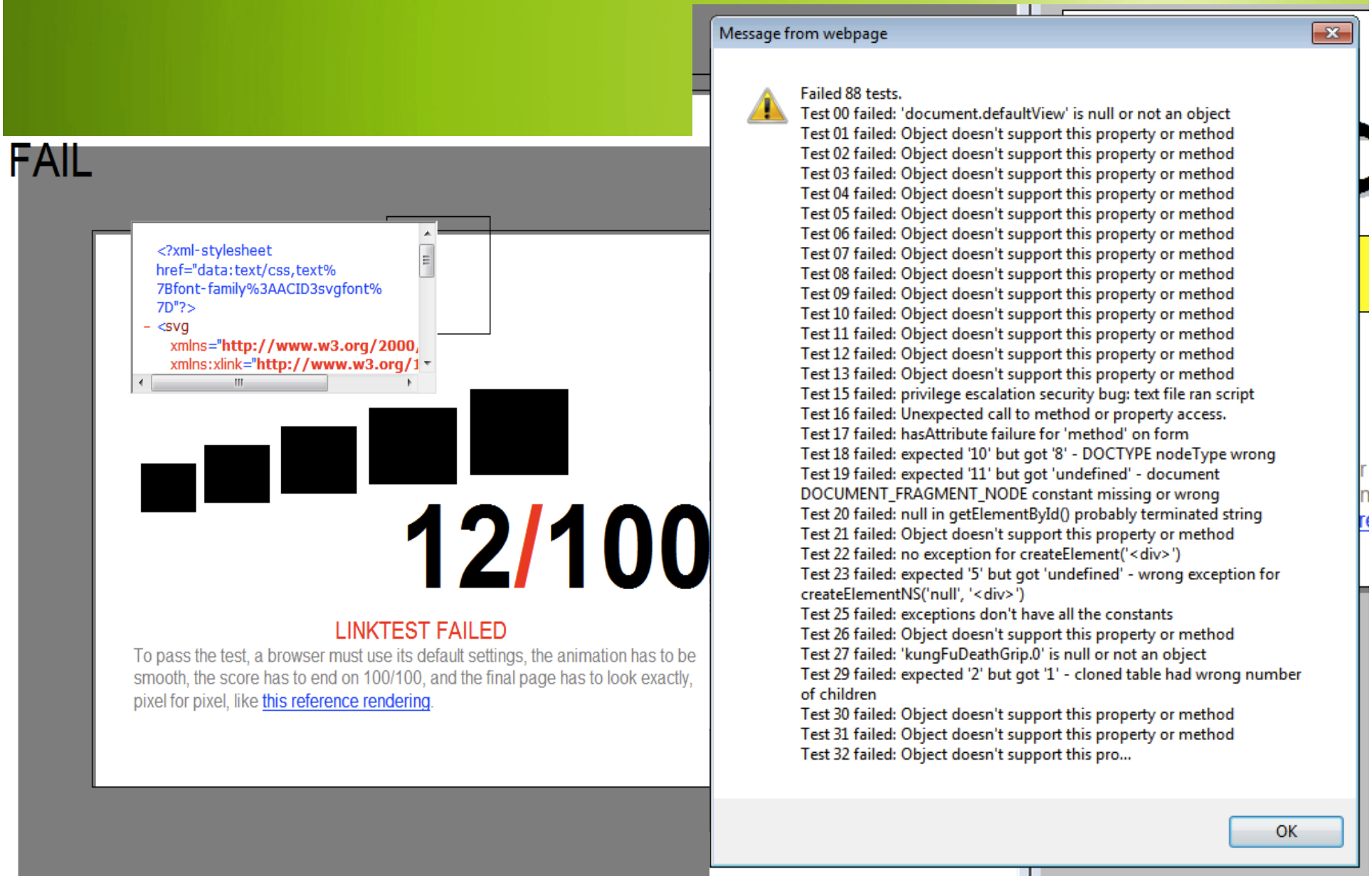
Internet Explorer 8

- Can be used on XP and Vista
- Better than IE 6 and 7
- SmartScreen
- XSS Filter
- Data Execution Prevention

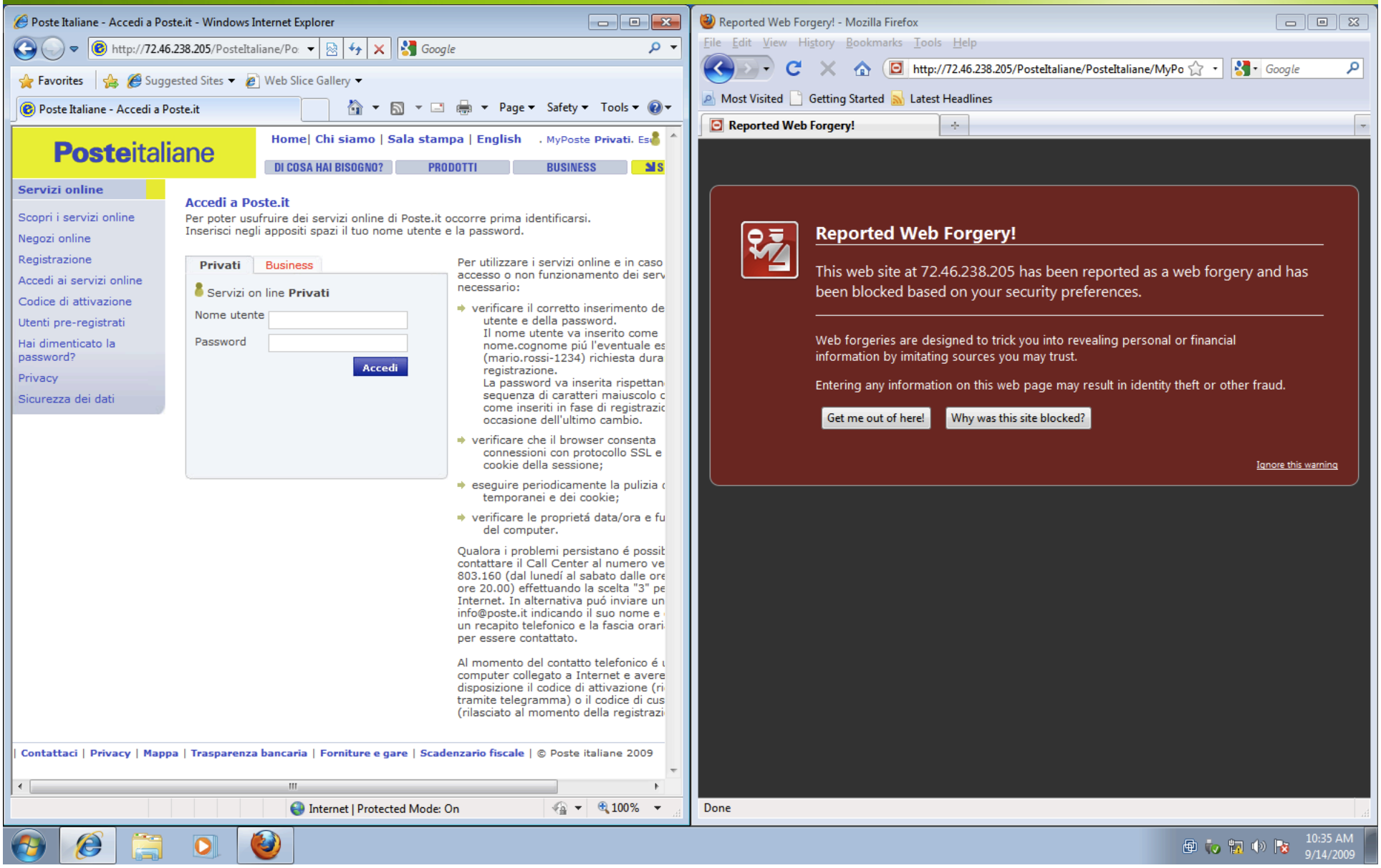
Internet Explorer 8 – Acid Test?



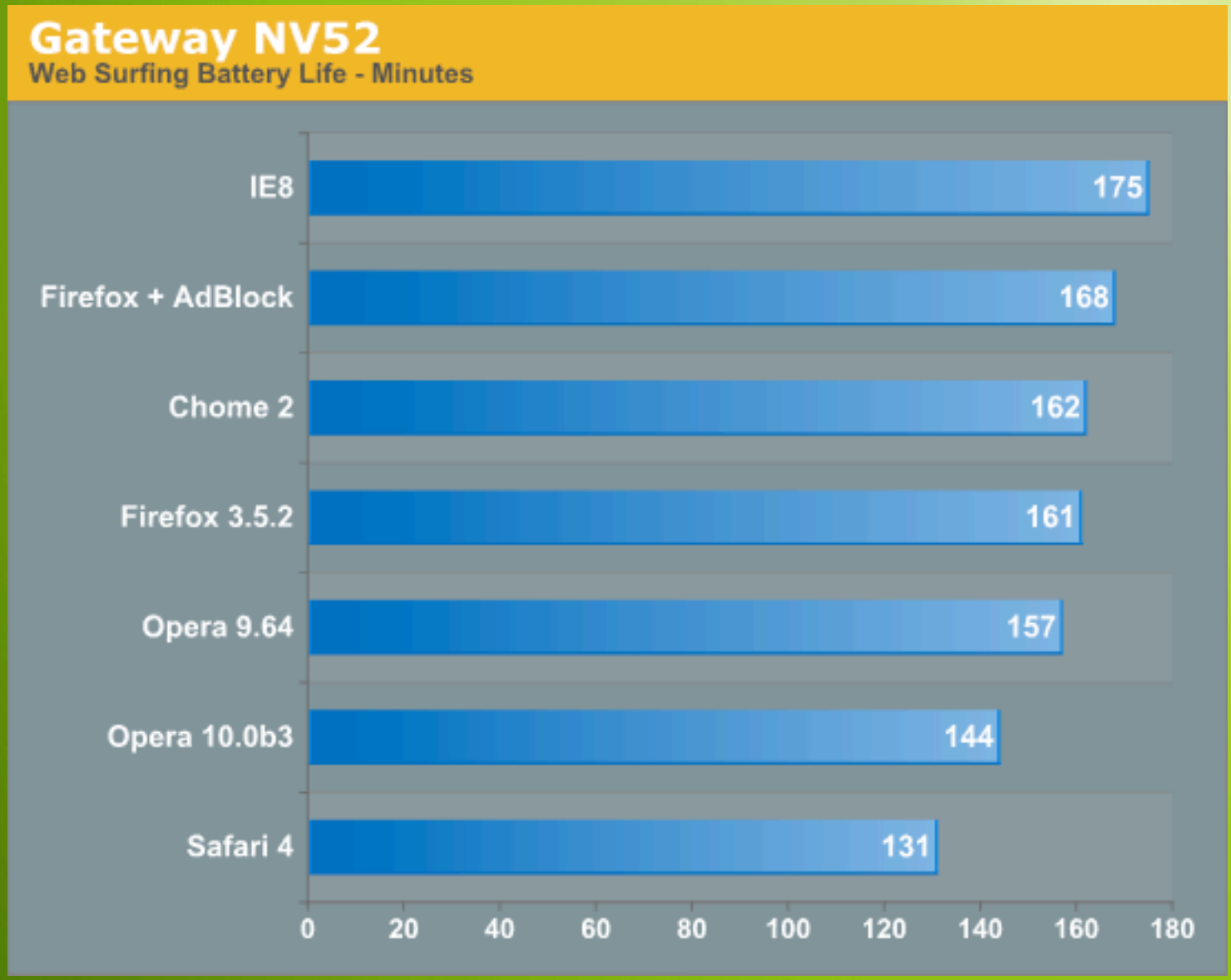
Internet Explorer 8 – Acid Test?



Internet Explorer 8 – SmartScreen?



Internet Explorer 8 – FTW?



http://bit.ly/17KT8I

XP Mode

- XP remains App standard
- Makes it easy to be compatible
- Don’t forget to secure this VM!

With Server 2008 R2

Windows 7 with Microsoft Windows Server 2008 R2 features:

- AppLocker
  - Application White Listing
  - Enforce App Standardization
- Branchcache
  - Caches files from WAN
- DirectAccess
  - No need for VPN
  - Easier for administration
  - Uses SSL, IPv6, IPSec
- Federated Search
  - Search all assets including SharePoint

Management

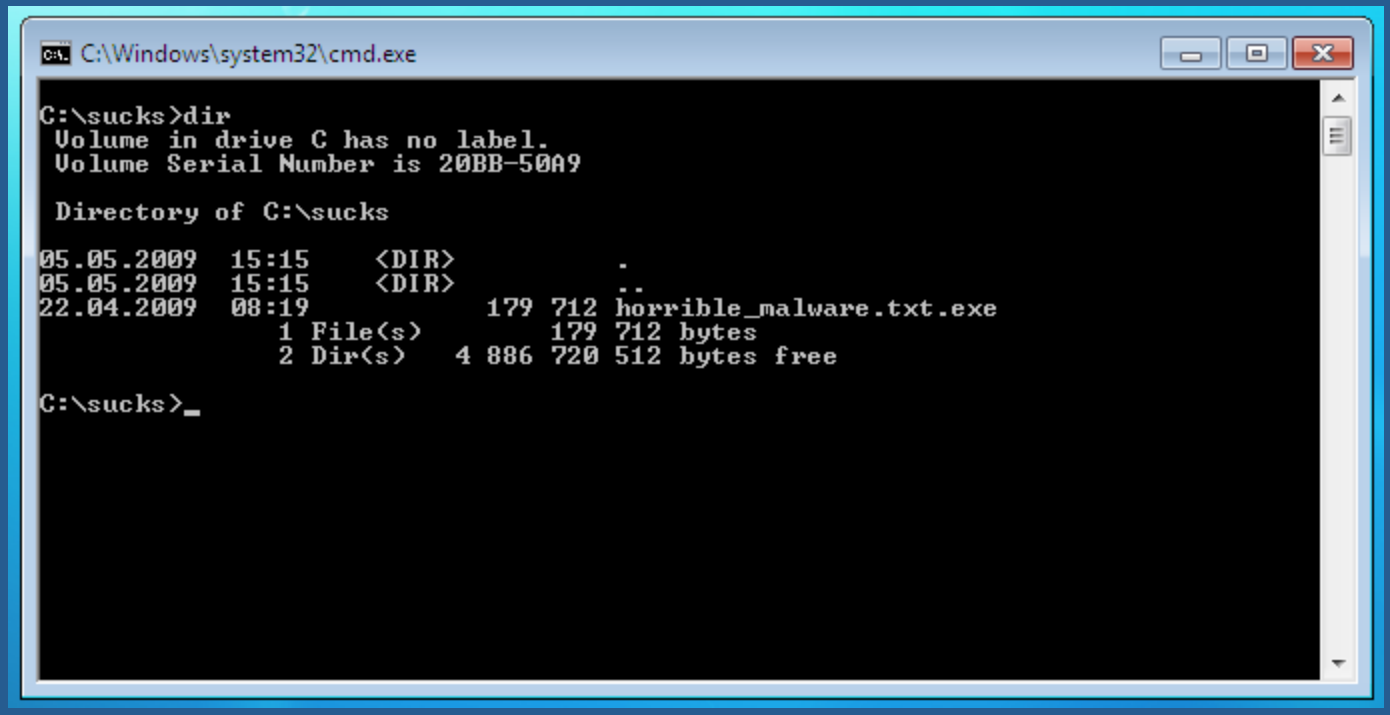
- PowerShell v2
  - IIS
  - Exchange
  - Cmdlets
  - Remote Management
- Enhanced Group Policy

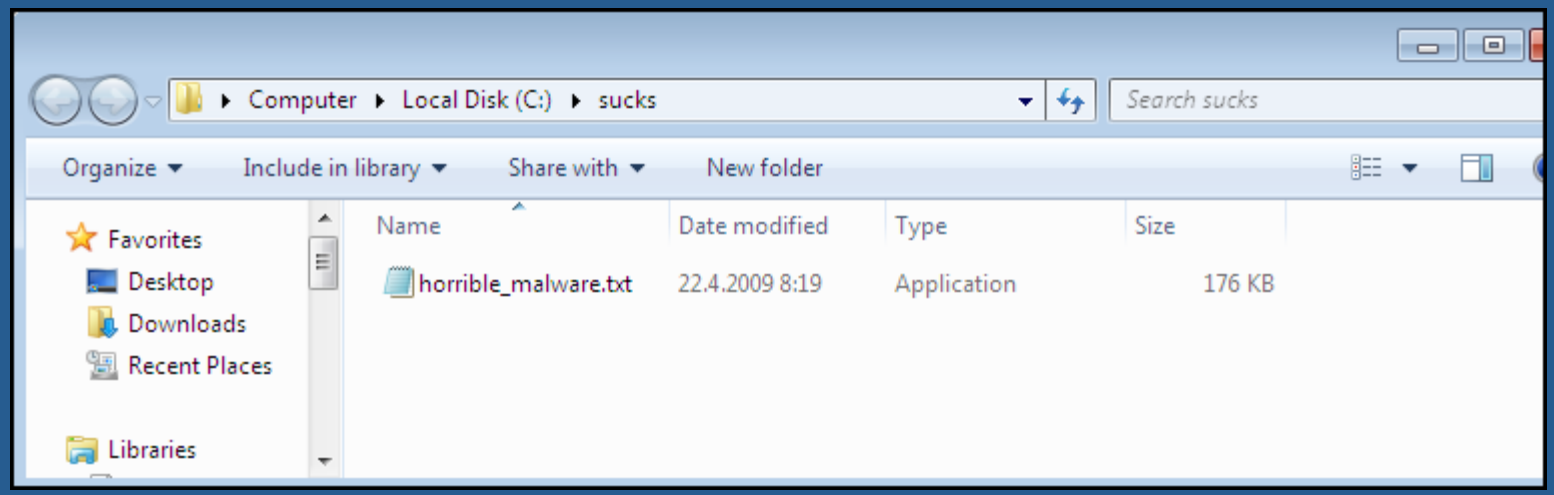
Secure?

- So far yes!
- September Patch Tuesday
  - None for Windows 7
- SMB2 0day?
  - Does not affect Windows 7 final

http://bit.ly/10ffcx

Hide extensions for known file types

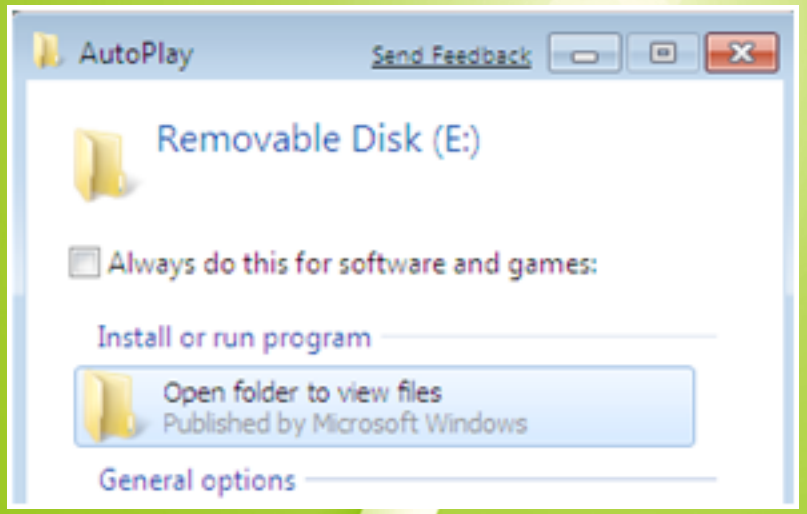


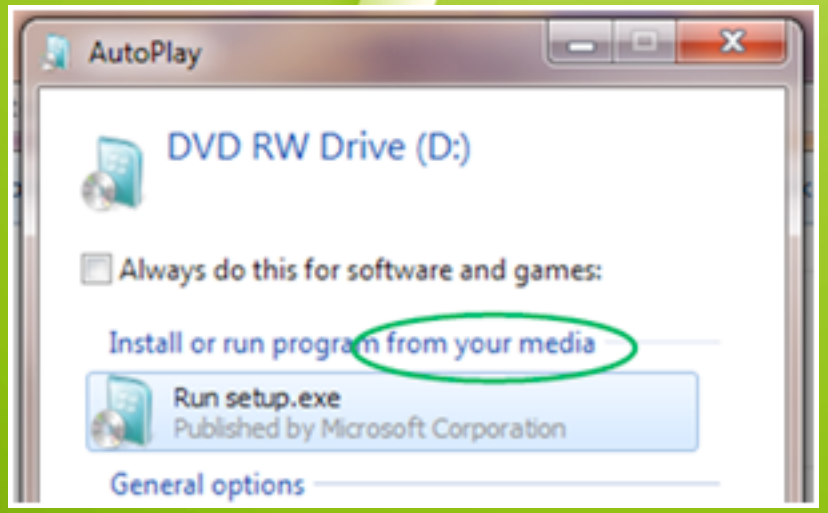


AutoRun

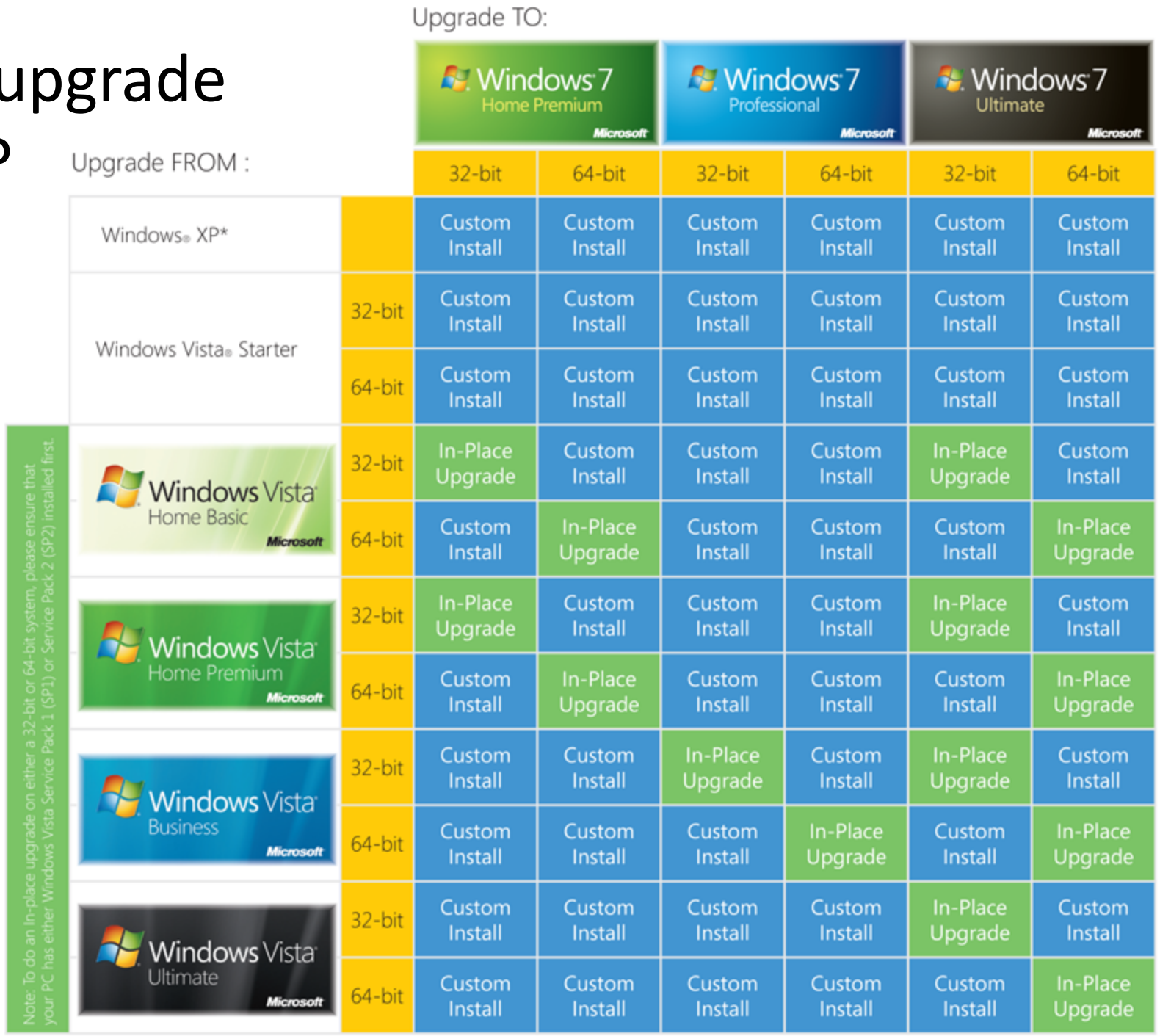
- No longer AutoRun/ AutoPlay with non-optical media
- Easier to distribute CD's than Flash Drives!
- Patch available for past OS

http://support.microsoft.com/kb/971029





Easy upgrade path?



Upgrade FROM :		Upgrade TO: Windows 7 Home Premium 32-bit	Windows 7 Home Premium 64-bit	Windows 7 Professional 32-bit	Windows 7 Professional 64-bit	Windows 7 Ultimate 32-bit	Windows 7 Ultimate 64-bit
Windows® XP*		Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
Windows Vista® Starter	32-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
Windows Vista Home Basic	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
Windows Vista Home Premium	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
Windows Vista Business	32-bit	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade
Windows Vista Ultimate	32-bit	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade

Note: To do an in-place upgrade on either a 32-bit or 64-bit system, please ensure that your PC has either Windows Vista Service Pack 1 (SP1) or Service Pack 2 (SP2) installed first.

Upgrade can take a full day!

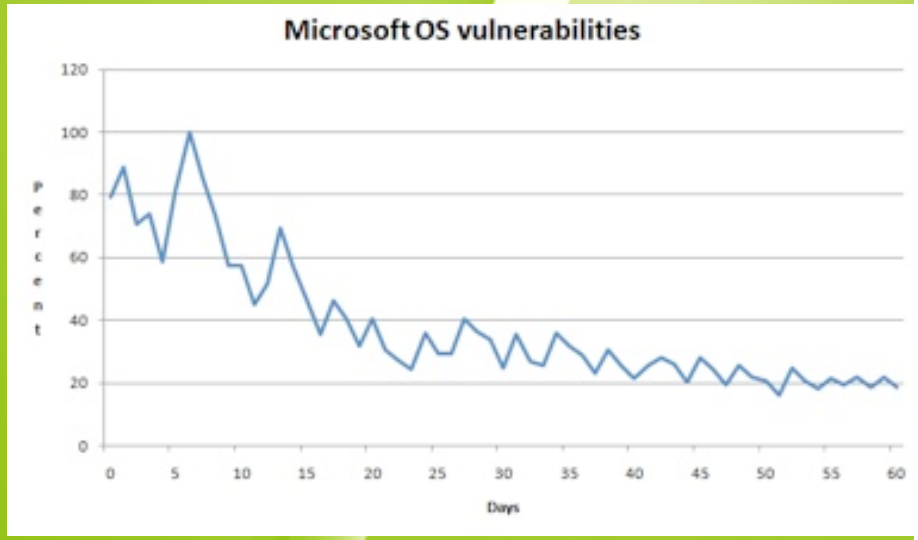
Data Profile	Low End Hardware	Mid End Hardware	High End Hardware
Clean No data and 0 applications	32-bit: 40 minutes 64-bit: 50 minutes	32-bit: 30 minutes 64-bit: 35 minutes	32-bit: 30 minutes 64-bit: 35 minutes
Medium User 70Gb of data and 20 applications	32-bit: 175 minutes 64-bit: 185 minutes	32-bit: 115 minutes 64-bit: 95 minutes	32-bit: 100 minutes 64-bit: 85 minutes
Heavy User 125Gb of data and 40 applications	32-bit: 345 minutes 64-bit: 355 minutes	32-bit: 185 minutes 64-bit: 165 minutes	32-bit: 160 minutes 64-bit: 150 minutes
Super User 650Gb of data and 40 applications	N/A	32-bit: 1220 minutes 64-bit: 675 minutes	32-bit: 610 minutes 64-bit: 480 minutes

http://bit.ly/39iiVt

Evolve

Cyber Crime Has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker(1); 1 in 5 Will Become a Victim(2)

- Cyber Crime is UP!
- Threats have evolved
  - Less platform-centric

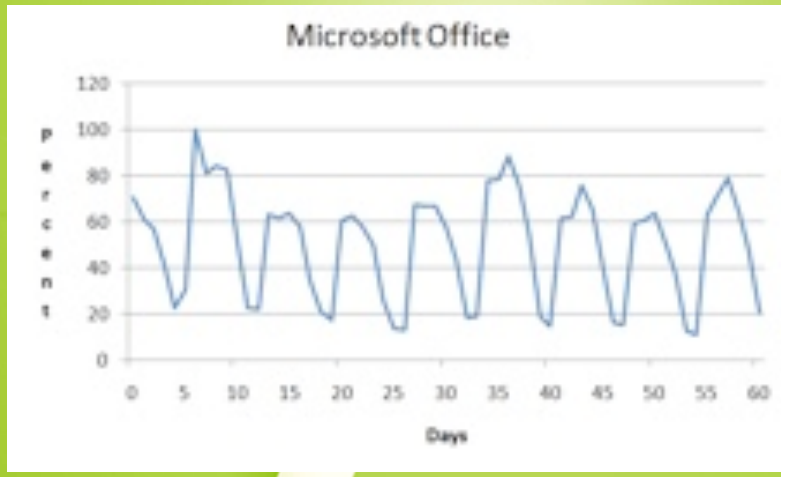


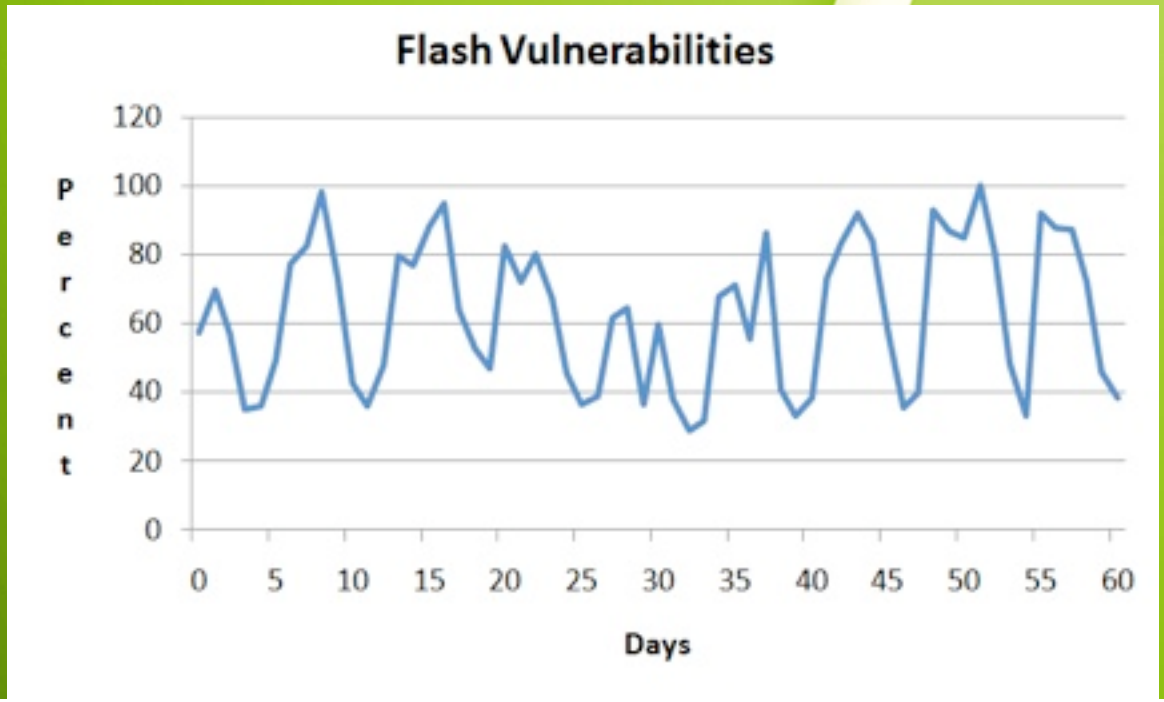
http://bit.ly/akwRT
http://www.sans.org/top-cyber-security-risks/

Windows 7

Evolve

- Attack the applications
- Attack the browsers
- Attack the users





Evolve – Stay Current

- Train Users!
  - Security Awareness
  - Browser Security
  - Windows Training?

Recap

- If you run Windows now, you will be on 7 eventually
- Secure it!
  - Educate Users
  - Use BitLocker or FDE
  - Patch Everything
  - Use AntiMalware
  - Use Firefox
    - no script - http://noscript.net/
    - WOT - http://www.mywot.com/

Recap

- Carefully plan migration from XP to 7
- Train users:
  - Security Awareness
  - Browser Use
  - Windows 7 training

Questions?

Thank You

Email: jorgeao@gmail.com

Blog: http://www.orchilles.com

http://www.twitter.com/
jorgeorchilles