FDCC and USGCB: Unmanaged to Managed

Highs and Lows from the Field

Presenters

Shelly Bird
shellybi@microsoft.com
Deployment Solutions Architect
Microsoft Consulting Services
Public Sector

CONTRIBUTORS
Microsoft Public Sector Deployment Teams

Agenda

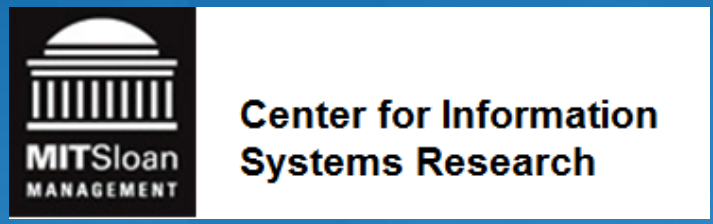
- Definitions
- What Matters
- Blockers and Stoppers
- What Works
- Why Managed?
- Geek Out

FDCC and USGCB

- Windows Desktops
- Security Settings
  - Windows XP
  - Vista
  - Windows 7
- Measurements
- Local User Rights
- Enterprise Standards

Definition of Managed

- Users run with User Rights
- Corporate standard for desktop and servers
- Standards *evolve*, but are:
  - Known at all times
  - Can be measured
  - Accountable



What Matters

Critical Elements for
Successful FDCC or USGCB Deployment

What Matters

Keep
It
Simple

'Simple' Requirements

Minimize Steps

Shorten Install Times

Blockers

- Data and Applications
  - Find
  - Sift
  - Transfer
- Image engineering
- Image distribution in challenged networks
- Image application re-provisioning
- Custom security lockdowns
- “Eco-System” impacting the standard

Stoppers

- Cowboy culture
- Hand crafting
- No app left behind

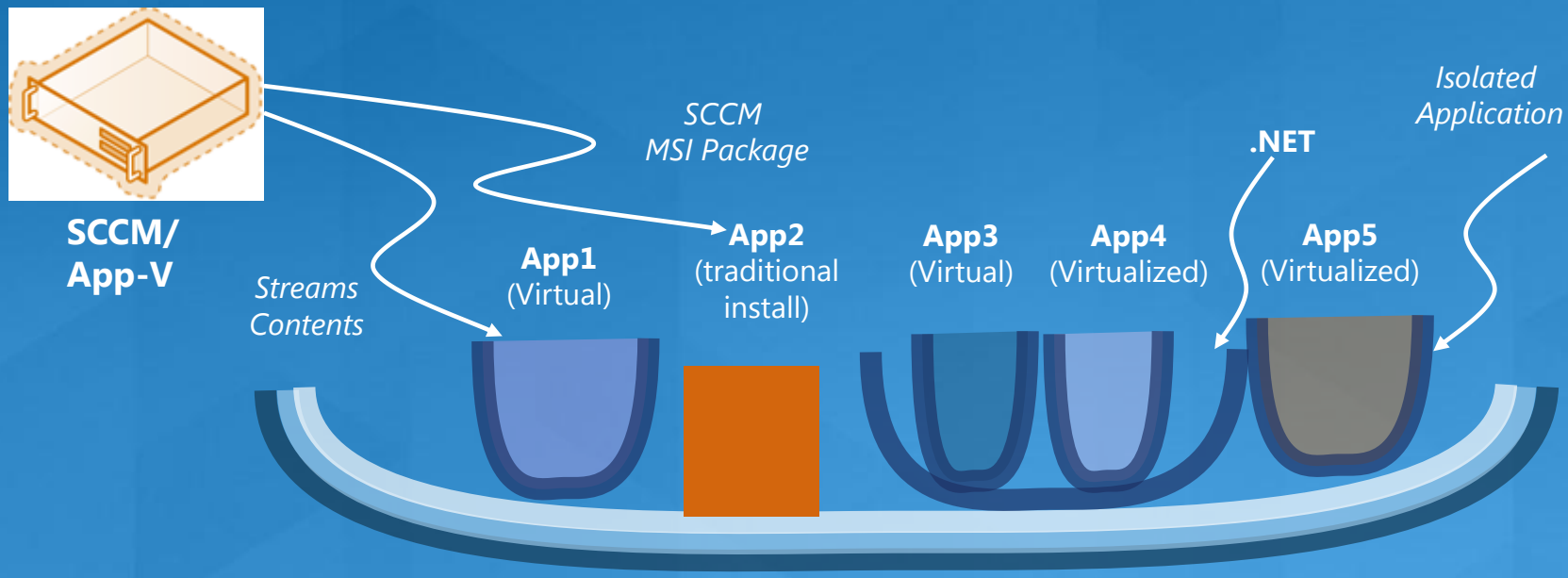
What Works: Dealing with the Blockers and Stoppers

The Dynamic Image (1)

- What it is NOT
- Image as a Container
- Hard exterior, mold the interior

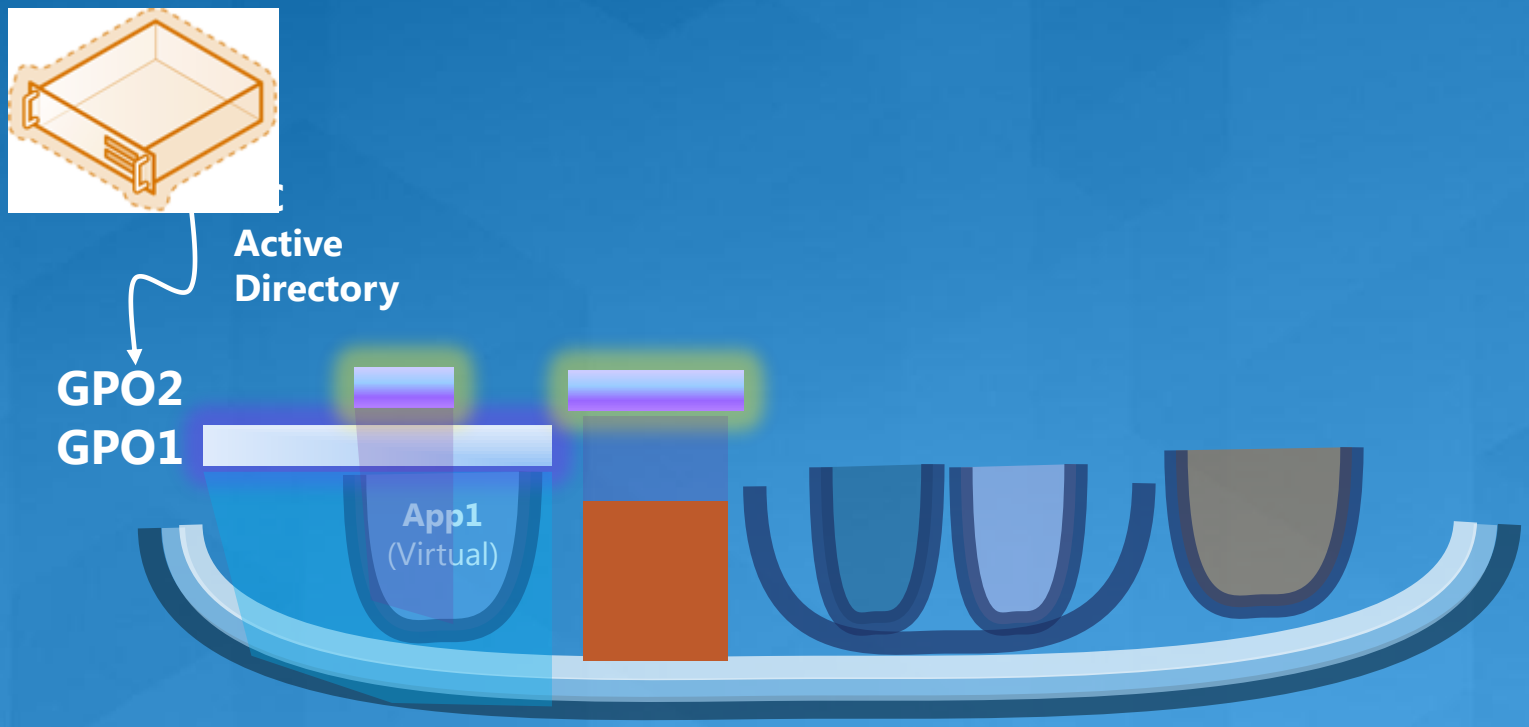
The Dynamic Image (2)

- Image contents: edits, applications



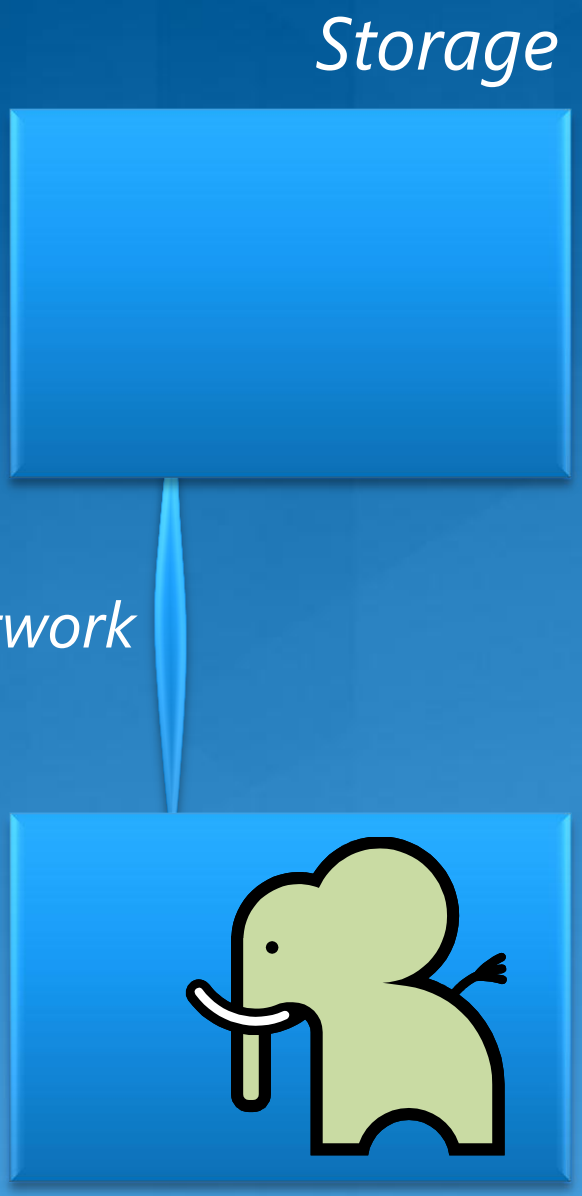
The Dynamic Image (3)

- Image contents: edits, applications
- Image layers: Group Policies (FDCC, USGCB)



Data

- **Find it.**
  - Vacuum cleaner approach
  - Depend on the Users
  - *Don't promise perfection*
- **Sift it.**
  - What needs encryption?
  - What needs backup?
  - What is not required?
  - *Set the enterprise standard*
- **Transfer it.**
  - User State Migration Tool (USMT)



Applications

- **Find it.**
  - Systems Mgt Reports
  - Stakeholder Lists
  - Installation media
    - Static Analysis
- **Sift it.**
  - Multiple versions
  - Duplicate functions
  - Target funding
- **Transfer it.** *Package*:
  - Priority applications
  - Fixes with application

Use the (Free!) Tools

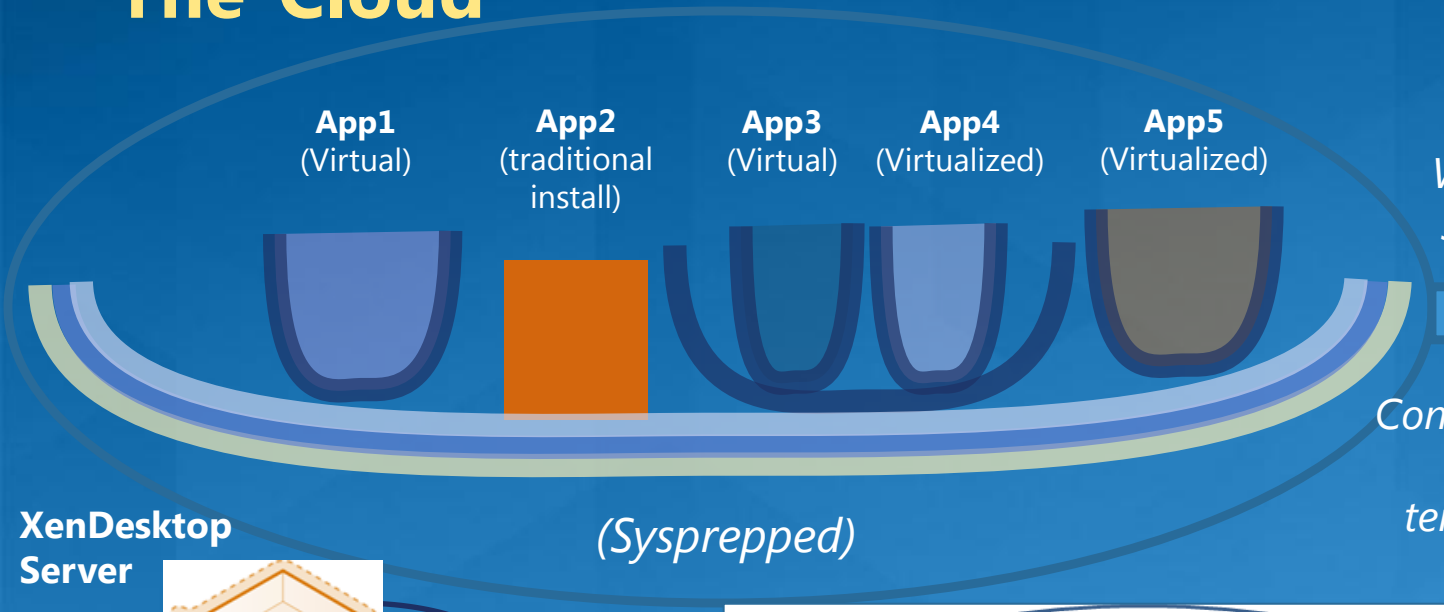
- Security Compliance Manager:
  - http://www.microsoft.com/downloads/en/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e&displayLang=en
- Sysinternals Process Explorer
  - http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
- Microsoft Deployment Toolkit Update 1 and User State Migration Toolkit 4.0
  - http://www.microsoft.com/downloads/en/details.aspx?FamilyID=3bd8561f-77ac-4400-a0c1-fe871c461a89

Why Managed Matters

Cloud, Security, Cost, Control

Why Managed Matters

The Cloud

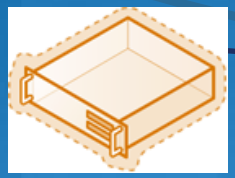


Capture With MDT or SCCM OSD

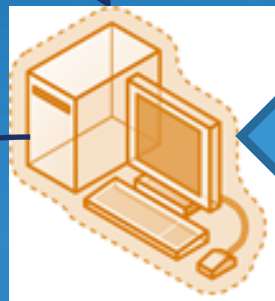
WIM Filecopy Image File (.WIM)

Convert to VHD template

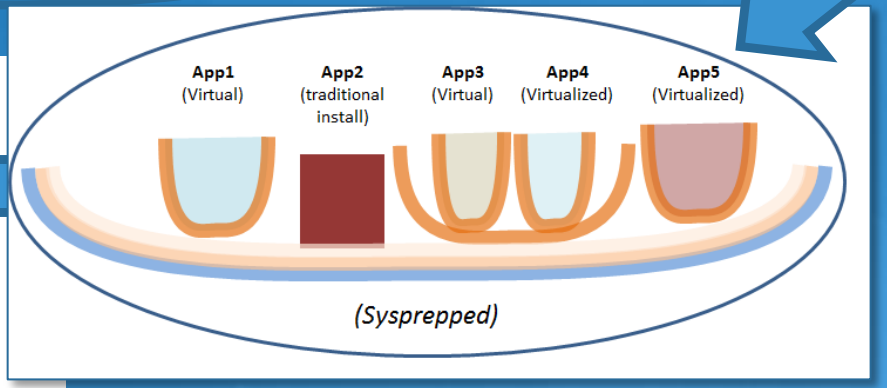
XenDesktop Server



Virtual



Windows 7 VDI VM
- Windows 7 Enterprise OS
- App-V 4.6 Client
- Citrix Receiver



Thin-Client Device
- Web Browser
- Citrix Receiver

Physical

Windows 7 Desktop PC
- App-V Client
- MED-V Client & XP VM
- SCCM Client Agent
- Citrix Receiver

Why Managed Matters

The Security Threat

Top Windows Malware 2H 2009			
	Family	**Category**	**Method**
1	**Win32/Taterf**	Worms	Autorun.inf in root of drives
2	**Win32/Renos†**	Trojan Downloaders & Droppers	Downloads and executes installation of other malware which load files into %ProgramFiles%
3	**Win32/FakeXPA***	Miscellaneous Trojans	Downloads and executes installation of other malware which load files into %ProgramFiles%
4	**Win32/Alureon†**	Miscellaneous Trojans	Downloads and executes installation of other malware; edits HKLM keys, attacks HW drivers
5	**Win32/Conficker†**	Worms	Attack on svchost.exe
6	**Win32/Frethog**	Password Stealers & Monitoring Tools	Inserts commands into registry Run keys, injects DLL into explorer.exe
7	**Win32/Agent**	Miscellaneous Trojans	Inserts commands into Run key, All Users Profile
8	**Win32/BaiduSobar**	Misc. Unwanted Software	HKEY_CLASSES_ROOT, installs files into %ProgramFiles%
9	**Win32/GameVance**	Adware	Installs malware into %ProgramFiles%, HKLM\Software
10	**Win32/Hotbar**	Adware	HKEY_CLASSES_ROOT, installs files into %ProgramFiles%

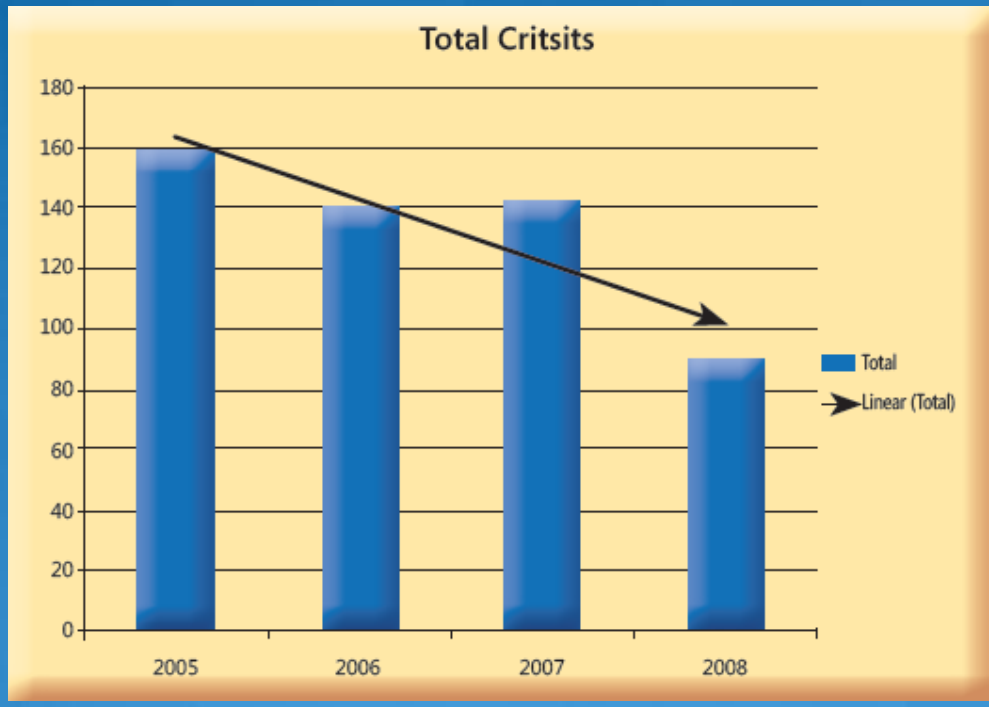
Microsoft Security Intelligence Report: http://download.microsoft.com/download/4/3/8/438BE24D-4D58-4D9A-900A-A1FC58220813/Microsoft_Security_Intelligence_Report%20_volume_8_Key_Findings_Summary_English.pdf

Why Managed Matters

Cost

US Air Force: *Saved $30M with Standard Desktop*

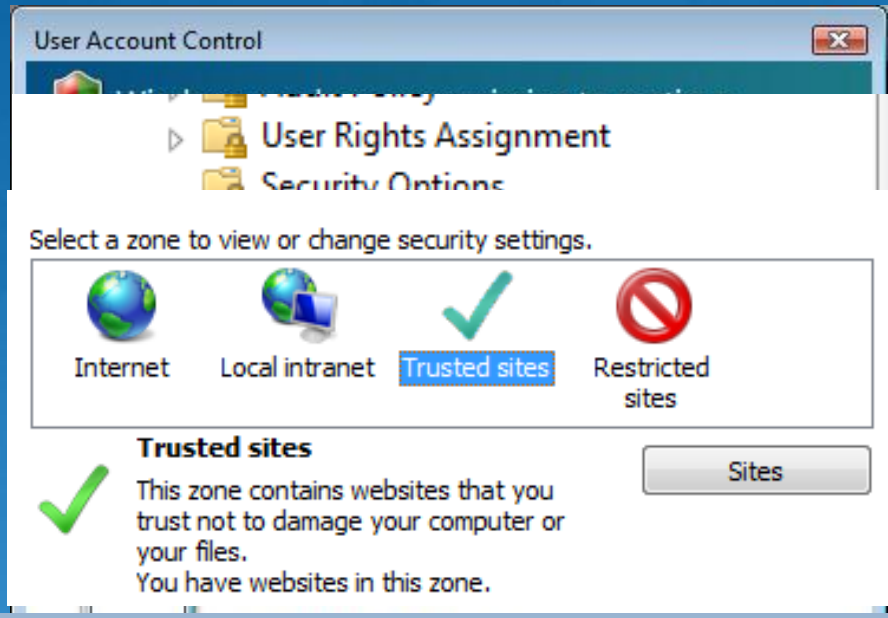
- 425,000 SDC desktops deployed in ten months
- 30% drop in local technical support resources without impacting mission
- Accelerated Technology Refresh cycles
- Security Incidents / Critsits dropped significantly

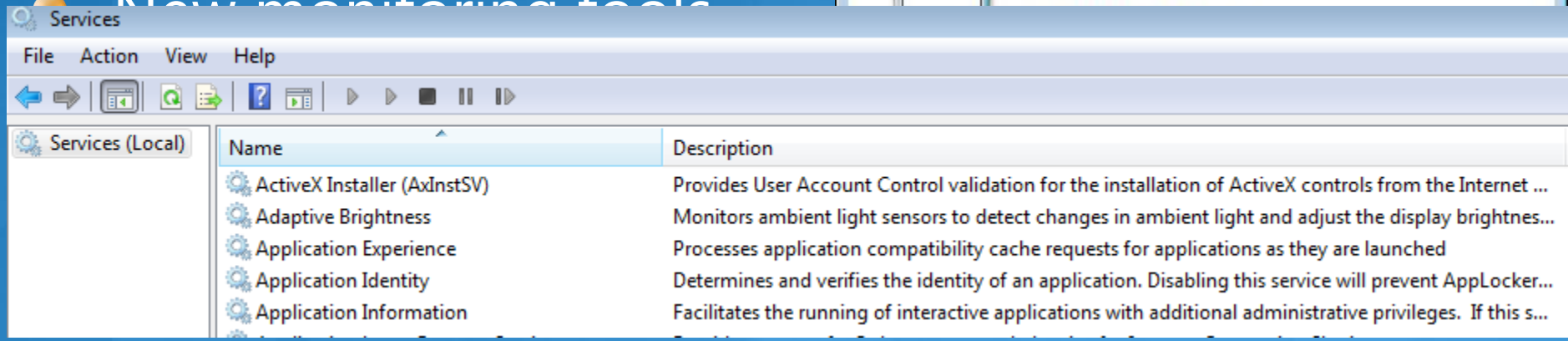


Why Managed is Possible

Control: User Testimonials or "Hey, it isn't *that* bad"

- UAC prompts are dropping drastically
- Creatures of habit
  - Outlook and Word
  - Firewall exceptions < 1 mo
  - Trusted sites < 2 mos
  - ActiveX Controls
- New monitoring tools





Why Managed Matters

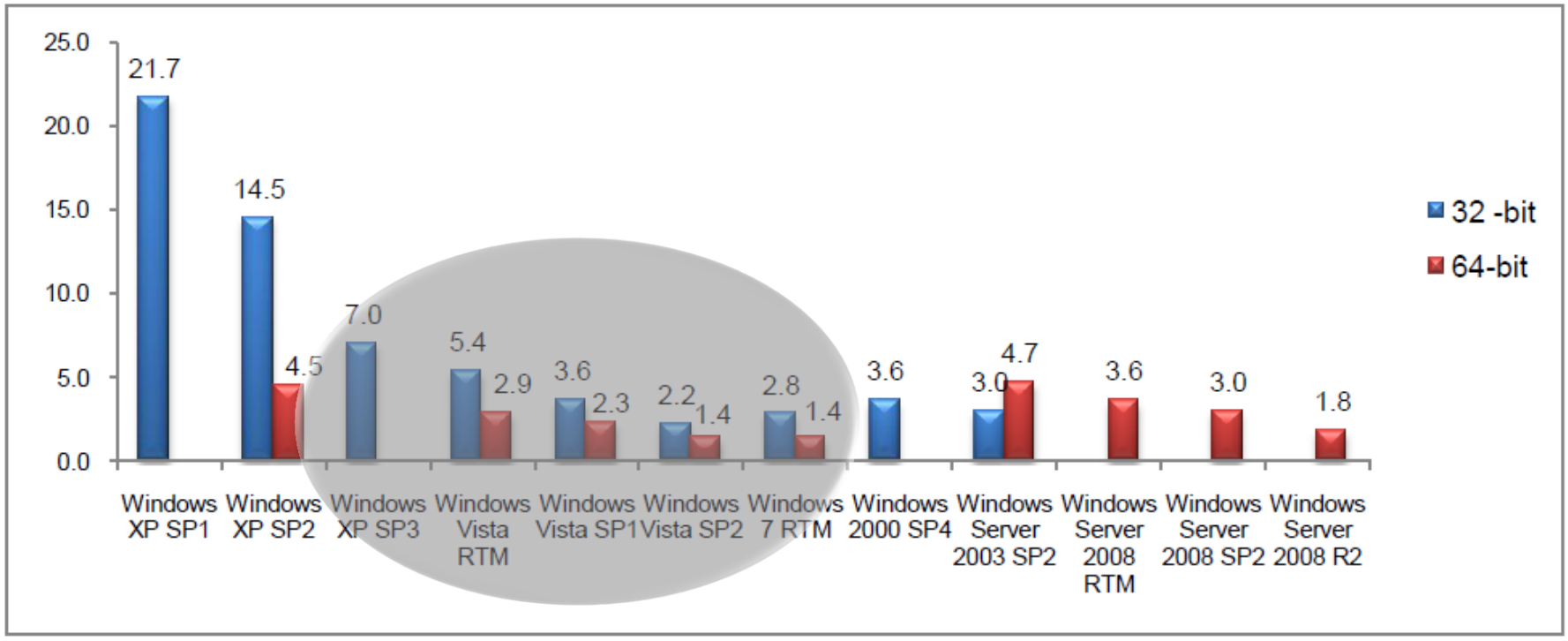
Control: Tales from the Field

- SPAM (mystery meat) configurations
- The case of the disappearing agent

Geek Out

Your OS Choice is Important

Figure 4: Number of computers cleaned for every 1,000 MSRT executions, by operating system, in 2H09



Microsoft Security Intelligence Report: http://download.microsoft.com/download/4/3/8/438BE24D-4D58-4D9A-900A-A1FC58220813/Microsoft_Security_Intelligence_Report%20_volume_8_Key_Findings_Summary_English.pdf

Top Six Fears with FDCC/USGCB

- **Firewall**
  - Inbound only
- **Plug-ins and add-ons**
  - In top demand: JRE, Adobe Reader, .NET
  - ActiveX Installation Service (AXIS)
- **FIPS Encryption**
  - Breaks less than people expect; worth fighting for
- **Internet Explorer 7 and 8**
  - End Run: users demand Firefox
  - Protected Mode: add site to Trusted Sites
- **Application Compatibility and Re-Provisioning**
  - Less impact with managed desktops compared to XP, due to User Access Control (UAC)
- **Printers**
  - Point and Print
  - Universal printer drivers

Some Issues: DHCP

- Vista and Windows 7 fail to obtain DHCP addresses when coming out of sleep mode
  - Default Firewall Unicast response settings block DHCP traffic; *Implement the predefined rule for Core Networking leaving only the "Dynamic Host Configuration Protocol (DHCP-in)" checked to allow DHCP communication for the Domain Profile*

Issues tracked and documented by Mike Cassidy, MCS Principal Consultant

Some Issues: IPv6

- DirectAccess and/or IPv6 dependent applications won't work
  - Default FDCC Disable ISATAP, Teredo, and 6to4 tunneling protocols via some registry entries; *if implementing DirectAccess or IPv6 set these registry settings to Enabled*

Issues tracked and documented by Mike Cassidy, MCS Principal Consultant

Some Issues: Certificates

- Certain applications won't install (e.g., Java Runtime Environment, etc.) since they use legitimate 3rd party certificates that are not pre-installed in a new image
  - Default FDCC / USGCB Turns off Automatic Root Certificates Update. Only major certificates are pre-installed in Vista/Win 7 to enhance performance, system assumes automatic root certificate updates will handle the rest, which it normally does. *Identify the 3rd party root certificate, publish certificate in Active Directory*

Issues tracked and documented by Mike Cassidy, MCS Principal Consultant

Common Issues: Wireless

- Mobile users can't use their wireless
  - WLAN AutoConfig: Disabled. *NIST provided guidance on their FDCC site for agencies who wish to use wireless on certain systems: must ensure all internal implementations of wireless use secure wireless (802.1x).*

Issues tracked and documented by Mike Cassidy, MCS Principal Consultant

Some Issues: IPSEC

- IPSec connections fail
  - FDCC limits Access this computer from the network to Administrators. When IPSec is used to provide session security, IPSec enforces network-based machine-authentication. For further details please see this FDCC blog post: http://blogs.technet.com/fdcc/archive/2008/10/21/fdcc-blog-alert-issue-with-windows-xp-vista-and-ipsec.aspx . *If IPSEC is utilized, add Authenticated Users or sub-groups that will be utilizing IPSEC security.*

References

- NIST FDCC and USGCB
  - FDCC http://fdcc.nist.gov
  - USGCB http://usgcb.nist.gov
- Core Infrastructure Optimization:
  - http://www.microsoft.com/infrastructure/
- MIT Center for Information Systems
  - http://cisr.mit.edu
- Microsoft Security Intelligence Report (SIR)
  - http://www.microsoft.com/security/about/sir.aspx
- Microsoft Malware Protection Center
  - http://www.microsoft.com/security/portal/Threat/Threats.aspx
- Contact Microsoft Public Sector FDCC / USGCB Team
  - kepage@microsoft.com
- Microsoft FDCC Blog
  - http://blogs.technet.com/fdcc
- Aaron Margosis Non-Admin Blog
  - http://blogs.msdn.com/b/aaron_margosis/
- Static Analysis Application Compatibility Scanning Tools
  - ChangeBase AOK http://www.changebase.com/
  - App-DNA http://app-dna.com/