NUIIT Tech Talk: Preview Windows Vista OS ready for a new day

Michael Greene
Client Technology Specialist
migreene@microsoft.com
Agenda

- Windows Vista Overview
- Windows Vista Security
  - Fundamentals
  - Threat and Vulnerability Mitigation
  - Identify and Access Control
  - Information Protection
- Desktop Optimization Pack for Software Assurance
- Question and Answers
Windows XP Offerings

- Windows XP Media Center Edition
- Windows XP Tablet PC Edition
- Windows XP Home Edition
- Windows XP Professional
- Windows XP Professional x64 Edition

- Windows Vista Starter Edition

Windows Vista Offerings

- Windows Vista Ultimate
- Windows Vista Home Premium
- Windows Vista Home Basic
- Windows Vista Enterprise
- Windows Vista Business
Windows Vista Overview

Find and use information

Improve security and compliance

End Users

Enable mobile workforce

Optimize desktop infrastructure

IT Pros
Windows Vista
Key Business Scenarios

Find and use information

End Users

Enable mobile workforce

- Search – start menu, control panel, document folder
- Metadata tags - easy to Search and Organize Your Data
- Tabbed browsing – IE7 and web printing
- ReadyBoost – USB extends memory
- Windows Aero – tabbed browsing
- High Performing, Reliable PC

- NAP – ensures secure state before connecting to the network (more secure)
- Easier to Connect, Collaborate, and Share
- Mobility center – puts most commonly used controls in one location
- Sync Center – data and devices switch between online and offline states
**Windows Vista**

Key Business Scenarios

- IE7 Protected Mode – prevents silent install of malicious code
- Services hardening – prevents windows services from being used for abnormal activity
- UAC – admin vs. standard
- Anti-phishing
- Group policy – easier desktop management
- Fundamentally Secure Platform
- Cost Effective Networking – automatically optimizes file transfers by detecting how much network bandwidth is available
- Support Costs = network diagnostics/built-in diagnostics for self healing
- Reducing Deployment Costs & Complexity

**IT Pros**

- Improve security and compliance
- Optimize desktop infrastructure
The Problem in A Nutshell

Hacker hits Georgia state database
Confidential information on more than 570,000 people exposed
Computerworld, March 2006

Ohio secretary of state sued over ID info posted online
Computerworld, March 2006

Hacker Breaks Into Nebraska Child-Support Database
SSNs for 300,000 people potentially impacted
Fox News, June 2006
Specific Business Challenges

- Keep systems secure from malware/spyware
  - Rootkits, keystroke loggers, bots
  - Worms, viruses
  - Phishing attacks
- Keep inside information inside
  - Lost/stolen laptops and desktops
  - Hacking
  - Accidental/intentional information leaks
  - Decommissioned/donated PCs
- Simplify identity and access management functions
Fundamentals
Securing the codebase and services
Security Development Lifecycle

**Product Inception**
- Assign security advisor
- Identify security milestones
- Plan security integration into product

**Design**
- Define security architecture and design guidelines
- Document elements of software attack surface
- **Threat Modeling**
- Standards, best practices, and tools
  - Apply coding and testing standards
  - Apply security tools (fuzzing tools, static-analysis tools, etc)

**Implementation**
- Security Push
  - Security code reviews
  - Focused security testing
  - Review against new threats
  - Meet signoff criteria

**Verification**
- Final Security Review
  - Independent review conducted by the security team
  - Penetration testing
  - Archiving of compliance info
  - RTM and Deployment

**Release**
- Security Response
  - Plan and process in place
  - Feedback loop back into the development process
  - Postmortems
**Windows Service Hardening**

**Defense in depth**

- Services run with reduced privilege compared to Windows XP.
- Windows services profiled for allowed actions to the network, file system, and registry.
- Designed to block attempts by malicious software to make a Windows service write to an area of the network, file system, or registry that isn’t part of that service’s profile.
Threat And Vulnerability Mitigation
Protect against malware and intrusions
Internet Explorer 7

Social Engineering Protections
- Phishing Filter and Colored Address Bar
- Dangerous Settings Notification
- Secure defaults for IDN

Protection from Exploits
- Unified URL Parsing
- Code quality improvements (SDLC)
- ActiveX Opt-in
- Protected Mode to prevent malicious software
Windows Defender

- Improved Detection and Removal
- Redesigned and Simplified User Interface
- Protection for all users
demo
Thwarting Malware
## Client Anti-Malware Offerings

<table>
<thead>
<tr>
<th>Feature</th>
<th>MSRT</th>
<th>Windows Defender</th>
<th>Windows Live Safety Center</th>
<th>Windows OneCare Live</th>
<th>Microsoft Forefront</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove most prevalent viruses</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Remove all known viruses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time antivirus</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove all known spyware</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time antispyware</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central reporting and alerting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>For Individual Users</th>
<th>For Businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>No charge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No charge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No charge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$50/3 PCs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TBD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Windows Vista Firewall

- Combined firewall and IPsec management
  - New management tools – Windows Firewall with Advanced Security MMC snap-in
  - Reduces conflicts and coordination overhead between technologies
- Firewall rules become more intelligent
  - Specify security requirements such as authentication and encryption
  - Specify Active Directory computer or user groups
- Outbound filtering
  - Enterprise management feature – not for consumers
- Simplified protection policy reduces management overhead
Group Policy Device Restriction
Identity And Access Control
Enable Secure Access to Information
User Account Control

Challenges

Most users run with full administrator privileges all the time
- At risk from malware
- Can’t manage desktops or enforce policy
- Expensive to support

Difficult to run a standard user
- User can’t perform many tasks
- Many applications don’t run

Windows Vista Solution

Easier to Run as Standard User
- Users can do more on their own
  - Change time zone, power settings, VPN, and more
  - Install approved devices
  - Admin commands clearly marked
- Higher application compatibility
  - File and registry virtualization

Greater Protection for Admins
- Software runs with lower privileges by default
- Administrator provides consent before elevation
Standard Users Can Do More

- View system clock and calendar
- Change time zone
- Configure secure wireless (WEP/WPA) connection
- Change power management settings
- Create and configure a Virtual Private Network connection
- Add printers and other devices that have the required drivers installed or allowed by IT policy
- Disk defragmentation is a scheduled background process
- Shield icon consistently marks what actions a standard user can and cannot do
demo
User Account Control
Improved Auditing

More Granularity

- New subcategories for Logon, logoff, file system access, registry access, use of administrative privilege

New Logging Infrastructure

- Easier to filter out “noise” in logs and find the event you’re looking for
- Tasks tied to events: When an event occurs, such as administrative privilege use, tasks such as sending an Email to an auditor can run automatically
“After virus infections, businesses report unintended forwarding of e-mails and loss of mobile devices more frequently than they do any other security breach”

Jupiter Research Report, 2004
Internal threats are just as prevalent as external threats. Here are the types of threats:

**Accidental**
- Loss due to carelessness
  - Careless forwarding of documents and Emails
  - Machine disposal or repurposing without data wipe
  - Data lost in transit
  - Confidential data copied via USB and other mobile devices

**Intentional**
- Data intentionally compromised
  - Untrusted network administrator accesses unauthorized data
  - Offline attack on lost/stolen laptop
  - Forwarding of internal-only Email and documents to external parties

**Targeted**
- Thief steals asset based on value of data
  - Branch office server containing directory or database
  - CxO or government official laptop or mobile device
  - Thief plugs external storage device into machine to copy data
BitLocker™ Business Value

- Full Volume Encryption enhances the security value of all registry, configuration files, paging files, and hibernation files stored on the fully encrypted volume
  - Encryption of the hibernation file
    - Protects against hibernation of laptop with sensitive docs open
- Destroying root key allows for the safe re-deployment of corporate hardware by making previous data inaccessible
  - Not an end-user feature
  - Strong interest in enterprise IT
- Recovery available to any customer with access to a phone and their Administrator
BDE offers a spectrum of protection allowing customers to balance ease-of-use against the threats they are most concerned with.

- **TPM Only**
  - "What it is.”
  - Protects against: SW-only attacks
  - Vulnerable to: HW attacks

- **Dongle Only**
  - "What you have.”
  - Protects against: All HW attacks
  - Vulnerable to: Losing dongle Pre-OS attacks

- **TPM +*PIN**
  - "What you know.”
  - Protects against: Many HW attacks
  - Vulnerable to: TPM breaking attacks

- **TPM + Dongle**
  - “Two what I have’s.”
  - Protects against: Many HW attacks
  - Vulnerable to: HW attacks

---

**Spectrum Of Protection**

**Ease of Use**

**Security**
Bitlocker™ Drive Appears In XP
Bitlocker™ Drive Appears In Vista
Linux Bitlocker volume errors
1. Fdisk reads partition table... thinks fve partition is ntfs
2. wrong fs type, bad option, bad superblock on /dev/sda2, missing codepage or other error
3. Primary boot sector is invalid, Not an NTFS volume
Deecommissioning

Normal versus "Force Recovery"

- Nothing
- Reformat drive
- Admin wipes drive

- Delete keys
Windows Imaging

Four major components

- The imaging format
  - The file structure that holds the image(s)
  - Install.wim and boot.wim

- Tools
  - Tools such as imageX to capture, edit the WIM files

- APIs
  - APIs to enable tools to manipulate WIM images

- Enabling technologies
  - File system filters, boot filters etc
Deployment Design Innovations

**Windows Imaging**
- File based format – hardware independent
- Non-destructive upgrades
- Multiple images in one WIM file – space and complexity benefits
- Single instanced and compressed – small size
- Bootable, serviceable – flexibility

**Modularization**
- Add/remove optional components – drivers, patches, languages
- Image customization to certain degree
- Higher reliability
- Language independence
- Consistency across phases

- Single worldwide image
- Offline image servicing

Reduce the number of images!
Windows Vista Information Protection

Who are you protecting against?

- Other users or administrators on the machine? EFS
- Unauthorized users with physical access? BitLocker™

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>BitLocker</th>
<th>EFS</th>
<th>RMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptops</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch office server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local <em>single-user</em> file &amp; folder</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local <em>multi-user</em> file &amp; folder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote file &amp; folder protection</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Untrusted network admin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote document policy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remote document policy enforcement

Some cases can result in overlap. (e.g. Multi-user roaming laptops with untrusted network admins)
Desktop Optimization Pack
The Next Generation of SA Technologies
Dynamic Desktop Solutions

Accelerate deployment and increase manageability
- Dynamically deliver the virtual application solution
  - Minimize application compatibility issues
  - Transform applications into centrally managed services available when and where needed
- Translating Software Inventory into business intelligence
- Powerful tools to accelerate desktop repair
- Enhancing group policy with change management

Microsoft SoftGrid: Application Virtualization
Microsoft Asset Inventory Services
Microsoft Diagnostic and Recovery Toolset
Microsoft Advanced Group Policy Management
Some organizations may benefit from just using Vista Business with minimal application compatibility testing.

Most Enterprise organizations require more formal procedures for application lifecycle, problem, change and asset management.

Many organizations require a more robust asset, application and end-to-end infrastructure administration definition.
Are You Ready for a New Day?

- Evaluate & Deploy today
- Return your Eval and get the products today!
- Over 50 partners in Partner Pavilion
- How can we help you? Give us feedback!
Thank You

www.microsoft.com/business/uslaunchevent200

Michael.Greene@microsoft.com
ready for a new day
Winter Quarter 2007 Tech Talks

Save the date!

February 7: Data Security at Northwestern

February 21: Support with NUIT

University Library, Forum Room, Noon – 1 p.m.