Microsoft Forefront Migration

Windows Admin Group Meeting
April 27, 2011

Kirk Soluk
kmsoluk@umich.edu
Decision

• The university’s license with McAfee for Windows anti-virus software expires in June, 2012

• The license will not be renewed
Direction

• *Microsoft Security Essentials* for personally owned machines

• *Microsoft Forefront Endpoint Protection* for institutionally owned machines
## Timeline of Key Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 06.01.11 | McAfee VirusScan no longer available for new end-user installs       | - End Users redirected to MSE for personally-owned machines  
- End Users redirected to Forefront for institutionally owned machines  
  • Encouraged to contact local IT Dept. first. |
| 12.30.11 | IIA no longer provides tech support for VirusScan (or MS products)   | - End-Users contacting Service Desk (4-Help) will get “Tier 1” support:  
  • Redirected to MS, Local IT Dept., Showcase  
- IT Pro’s rely on existing Windows Support infrastructure:  
  • Peer support via Windows 2000 alias  
  • Premier support (if you have it)  
  • Per-incident (credit card) support from MS |
| 6.30.12  | Internal Signature Updates for VirusScan no longer provided          | Anyone still running a version of VirusScan configured to hit internal update servers at risk (includes VirusBuster’s UM package) |
Forthcoming Communications

• Email
  – Targeted announcement to IT Pros: FLN, Windows Admin, SecCom, ACSF, SAVU, anti.virus.sysadmins, etc.
  – Template email series for IT Pro’s to distribute within their units

• Print
  – New Student Orientation Publications
  – RESCOMP Presentations
  – URecord Article

• Web
  – New online resource to be established on safecomputing.umich.edu:
    • Who, What, When, Where, How for a/v
    • Virusbuters, BlueDisc and other web sites redirected to new web site
  – Recurring messages on CTOOLS, WA, ResComp Tip of the Day, ITS.umich Tout

• Marketing
  – Recurring advertisements on digital signs in Sites and Unions
FAQ in your Email

- What decision has been made regarding a/v at UM?
- Who made the decision?
- Why was the decision made?
- When does the McAfee license expire?
- When should I migrate?
- How long will the VirusScan software be available?
- What should I migrate to?
- What is the difference between MSE and FF?
- Where do I get MSE?
- Where do I get Forefront?
- Do I have to uninstall McAfee to install MSE or FF?

- Do I need a key to activate MSE or FF?
- Can MSE be installed on University-owned systems?
- Is AD required to install Forefront?
- Is SCCM required to install Forefront?
- Can Forefront be installed on Servers?
- How will support be provided?
- Where can I learn more?
- What is the replacement for ePO?
- Will ITS be providing a campus-wide SCCM service?
- Will ITS be releasing a customized installer for McAfee VirusScan 8.8?
- Do I have to use Forefront?
- What about anti-virus for Macintosh systems?
FAQ in your Email

- What decision has been made regarding a/v at UM?
- Who made the decision?
- Why was the decision made?
- When does the McAfee license expire?
- When should I migrate?
- How long will the VirusScan software be available?
- What should I migrate to?
- What is the difference between MSE and FF?
- Where do I get MSE?
- Where do I get Forefront?
- Do I have to uninstall McAfee to install MSE or FF?
- Do I need a key to activate MSE or FF?
- Can MSE be installed on University-owned systems?
- Is AD required to install Forefront?
- Is SCCM required to install Forefront?
- Can Forefront be installed on Servers?
- How will support be provided?
- Where can I learn more?
- What is the replacement for ePO?
- Will ITS be providing a campus-wide SCCM service?
- Will ITS be releasing a customized installer for McAfee VirusScan 8.8?
- Do I have to use Forefront?
- What about anti-virus for Macintosh systems?
How will support be provided?
(From an ITS perspective)

• ITS Service Desk (4Help) will provide very basic “Tier 1” support for End Users. Beyond that:

• End Users
  – Running Microsoft Security Essentials?
    → Visit MSE Support Portal
  – Running Microsoft Forefront?
    → Contact local IT department, No IT department?
    → Contact Microsoft Consumer Security Support Center
  – If that doesn’t work:
    → Visit the Computer Showcase (charges may apply)

• IT Pros
  – Windows 2000
  – Premier Support from MS (if you’ve paid for it)
  – Per Incident (credit card) Support from MS
Where can I Learn More?

• The FAQ has several links:
  – Forefront Web Site
  – Datasheet
  – Whitepaper
  – Evaluation Guide
  – Preconfigured VHD’s (Virtual Hard Disks) for evaluating Forefront
  – Video Demo – FEP Policy Management via SCCM.
  – Video Demo – FEP Protection Features
  – Technet Library
  – Microsoft Security Essentials Web Site
  – Microsoft Safety and Security Center
  – Manually Downloading Definition Updates for MSE
Where can I learn more?

• Slides from recent MMS conference
  – BI01 Advanced Malware Threat Detection and Removal with Forefront Endpoint Protection 2010
  – BI02 Forefront Endpoint Protection Overview Managing desktop security and antimalware solution with System Center Configuration Manager
  – BI04 Integrating Management & Security at Microsoft Forefront Endpoint Protection 2010 deployment case study at Microsoft
    – \its-files.m.storage.umich.edu\its-files\is\wids\di\MMS_2011_Sessions

• Obtain the Forefront Media from SWLD
  – https://www.itcs.umich.edu/sw-info/microsoft/products/
  – Use FEPInstall.exe for standalone deployments
# The Migration has Begun

<table>
<thead>
<tr>
<th>Unit</th>
<th>Current Status</th>
<th>Future Plans/Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus Comp. Sites</td>
<td>Union Site (at a minimum) by end of spring term</td>
<td>All sites running FF by start of Fall term; Initially manage by GP, then via SCCM</td>
</tr>
<tr>
<td>College of Engineering</td>
<td>1200 (lab) machines currently running FF</td>
<td>Migrate 600 Administrative Desktops by ???</td>
</tr>
<tr>
<td>Housing</td>
<td>Testing:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Student quarantine network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Internal deployment/management options</td>
<td></td>
</tr>
<tr>
<td>Housing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS</td>
<td>Testing Forefront Extensions to SCCM</td>
<td>Pilot clients in May; Complete migration by August</td>
</tr>
<tr>
<td>Law School</td>
<td>20% of machines currently running FF; Managing via GP</td>
<td>Remaining 80% of FAC/STAFF machines by end of calendar year 2011</td>
</tr>
<tr>
<td>Library</td>
<td>300 machines currently running FF; Managing via GP</td>
<td>Large capital replacement cycle in May (W7 + FF); Remainder of machines by end of calendar year.</td>
</tr>
<tr>
<td>LSA</td>
<td>Over 500 machines currently running FF; Infected machines being migrated during cleanup FF GPO on LSA OU; Push (SCCM) and Pull (custom) technologies made available to departments;</td>
<td>In process of establishing college-wide timeline</td>
</tr>
<tr>
<td>Shrd Dsktp.</td>
<td>Forefront has been approved.</td>
<td>W7 + FF available July 1st.</td>
</tr>
<tr>
<td>UMHS</td>
<td>Learning, Testing, Benchmarking; SCCM infrastructure already in place</td>
<td>Assuming tests pass, Migration complete by September, 2011</td>
</tr>
</tbody>
</table>
Action Items

• Read the FAQ
  – Give us feedback (its.iia@umich.edu)

• Hop on the migration bandwagon
  – Spread the word in your unit
  – Develop your migration plan and timeline
    • Shoot for the end of calendar year 2011
  – Help others that are migrating
Questions?