Kirkwood Community College Antivirus Evaluation
Purpose

• To ensure the top level of protection against growing virus and malware threats
• To reduce the number of hours spent manually cleaning infected machines across campus
• To minimize the level of end user involvement in the virus/malware process, thus improving the proactivity of the IT department
Candidates

- ESET Nod32 Enterprise Edition
  - [http://www.eset.com](http://www.eset.com)
- McAfee Active VirusScan
  - [http://www.mcafee.com](http://www.mcafee.com)
- Trend Micro NeatSuite
  - [http://www.trendmicro.com](http://www.trendmicro.com)
Needs

- Centrally managed system with the ability to deploy the antivirus client to the enterprise
- Reporting system that allows for notification of outbreaks and out of date clients
- Automatic updating of clients and servers
Wants

- Bundled protection against malware other than viruses
- A configurable notification and reporting system
- Multi-platform solution
- Proactive malware detection
# Need/Want Breakdown

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Centrally Managed</th>
<th>Deployable</th>
<th>Reporting</th>
<th>Auto Updates</th>
<th>Outbreak Notification</th>
<th>Bundled Malware</th>
<th>Configurable Reporting and Notification</th>
<th>Multi-Platform</th>
<th>Proactive Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nod32</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N</td>
</tr>
<tr>
<td>McAfee</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N</td>
<td>X</td>
<td>X</td>
<td>N</td>
</tr>
<tr>
<td>Trend</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
Preliminary Research

- Virus Bulletin.com, an independent, and internationally recognized malware advice and benchmarking website has provided the following comparison for our three candidates:

- **VB100% Results Overview: Eset Nod32**
  
  ![Bar Chart]
  
  40 Success / 3 Failure / 5 No Entry

- **VB100% Results Overview: McAfee**
  
  ![Bar Chart]
  
  28 Success / 18 Failure / 2 No Entry

- **VB100% Results Overview: Trend Micro**
  
  ![Bar Chart]
  
  15 Success / 7 Failure / 26 No Entry
Preliminary Research (cont)

- Independent study conducted by Virus Bulletin.com using common malware threats

<table>
<thead>
<tr>
<th>Worm Outbreaks</th>
<th>ESET NOD32</th>
<th>McAfee</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Detection Rate (%)</td>
<td>87%</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td>Number Detected out of 15</td>
<td>13</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comprehensive Protection</th>
<th>ESET NOD32</th>
<th>McAfee</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Anti-Threat Engine - protects against viruses, spyware, adware, identity theft</td>
<td>Yes</td>
<td>No, multiple components required in a large suite.</td>
<td>No, multiple components required in a large suite.</td>
</tr>
<tr>
<td>VB100% Awards for detection of all in-the-wild viruses in the VB test sets, and without any false-alarms. (virusbulletin.com)</td>
<td>39</td>
<td>26</td>
<td>14</td>
</tr>
</tbody>
</table>
Preliminary Research (cont)

- Independent study conducted by Virus Bulletin.com using common malware threats

<table>
<thead>
<tr>
<th>Comprehensive Protection</th>
<th>NOD32</th>
<th>McAfee</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed In-the-Wild Viruses in Virus Bulletin tests between May 1998 and May 2005 (virusbulletin.com)</td>
<td>2</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Real-time protection against 16 zero-day viruses (source: virustotal.com)</td>
<td>88%</td>
<td>31%</td>
<td>0%</td>
</tr>
<tr>
<td>Retrospective/ProActive Test by AV-Comparatives.Org on 3-month old signatures. Combined trend of May and November 2005 tests. (<a href="http://www.av-comparatives.org">www.av-comparatives.org</a>)</td>
<td>85%</td>
<td>20%</td>
<td>10%</td>
</tr>
</tbody>
</table>
Preliminary Research (cont)

- Independent Study conducted by Colby-Sawyer College

![Viruses Detected](chart.png)
Preliminary Research (cont)

- Independent Study conducted by Colby-Sawyer College
Preliminary Research (cont)

- Independent Study conducted by Colby-Sawyer College

![Bar Chart]

Amount of memory used when resident protection is idle

- F-secure, 31.5
- Etrust, 31
- McAfee, 31
- PC-Cillin, 28
- RAV, 26.5
- Norman, 26
- Norton, 23
- Kaspersky, 23.5
- Bit Defender, 17
- Nod32, 13.5
- F-Prot, 7

Megabytes of Ram used

- Panda, 55.5
Evaluation Phases

• Testing will be rolled out in two phases:
  – Time frame will be determined by length of trials obtained
  – Alpha Phase
    • Side by side stress testing in 105 KH
    • Approximately one week in duration
  – Beta Phase
    • “Real world” testing in a lab setting (potentially Allsop Computer Lab)