

Report on Anti-Virus Evaluation Testing and Recommendation

November 19, 2008

The enormity and complexity of virus and malware threats to computer end-users have changed dramatically since McAfee was chosen as the Anti-Virus solution for the University in 2001. Because of this, the VPT wanted to perform some due-diligence by evaluating other Anti-Virus products before the current McAfee contract expired. As a result, the Anti-Virus Evaluation Committee was formed from members of the VPT. The committee was charged with evaluating leading AV solutions in the marketplace and determining whether Auburn University should continue with the McAfee solution. Committee members were Bill Lacy (Chairperson – VetMed), Michael Chesnutt (Liberal Arts), Jonas Bowersock (ACES/Ag), Todd Chaloupka (OIT), Dudley Dent (OIT), Bill Henson (VetMed) Gerry Hicks (OIT), Jeff Walker (College of Engineering), Asim Ali (College of Education), Walter Tolbert (College of Human Sciences), Adam Williams (College of Business) and Mark Wilson (OIT). In addition to these members, Gerrit Dewitt assisted with Mac testing and Scott Lowery and Matt Riggs participated in product testing.

The committee's goal was to evaluate "best of breed" AV products (which included McAfee) and determine if it was beneficial for AU to switch to another solution. Below is a brief outline of the committee's tasks and procedures.

- Gathered a list of AV vendors from each committee member's knowledge and experience, web info, independent studies of AV products, and known industry leaders.
- Selected what we believed to be the top AV vendors: McAfee, Symnatec, Sophos, Kaspersky, TrendMicro, F-Secure and AVG.
- Developed a list of criteria/features to evaluate.
- Listened to each vendor present their product and how it would address the committee's criteria/feature list.
- Eliminated F-Secure because it was based in part on multiple scanning engines, was not a robust enterprise product, and was too bloated with features not included in our criteria.
- Eliminated AVG because it did not have enterprise management capabilities and lacked direct support from the manufacturer.
- Chose Sophos, TrendMicro, Kasperksy, and Symantec for further evaluation after hearing all of the presentations.
- Obtained trial versions of each remaining vendor's primary enterprise anti-virus product, and installed the management consoles as a group. The products were available to the entire committee for testing and OIT provided test management consoles for committee members that did not have their own.
- Set up each product's enterprise solution in Liberal Arts and CVM. Comparison testing was done on XP systems by Michael Chesnutt, Dudley Dent, and Bill Henson. Although there were some unexpected results in overall test times, all products performed better than McAfee.
- Eliminated Kaspersky because the home license price structure was convoluted and users would have to install an entirely different product than the enterprise version. In addition, the committee could only locate one other U.S. university using the product. Also, there

were some concerns over the unstable relationship between the countries of Georgia (Kaspersky's headquarters). and Russia

- Chose Symantec, Sophos, Trend, and McAfee as the final four products.
- Eliminated Symantec because the management console was very cluttered and unnecessarily complicated.
- Eliminated Trend because of the lack of an "in-house" Mac product, the fact that the home use product would be entirely different than the enterprise solution, and the dislike of the management console interface.
- Placed reference calls to The University of Arizona, St. Louis Public Schools, Escambia County Schools, and Miami/Dade School District to further evaluate Sophos. All customers indicated that they were very satisfied with the product and the quality of Sophos's support.
- Answered all committee member's questions and concerns about the final four products.
- Asked Sophos to provide the committee with implementation/product replacement recommendations.
- Voted on the 1st and 2nd choice for an Anti-Virus Product out of the final four products: Sophos, Trend, Kaspersky, and Symantec.

Because everyone on the committee wears many hats, we were not able to dedicate as much time to the evaluation as we would have liked, but we are confident the process was thorough enough to make a recommendation. [The Anti-virus Evaluation Committee recommends Sophos as Auburn University's Anti-Virus Solution when the McAfee contract expires \(June 8, 2009\).](#)

It is the Committee's opinion that the benefits of switching to Sophos will be:

1. Significantly better support from the vendor.
2. Improved distributed management across campus computing environments.
3. More effective prevention and removal of virus and spyware threats.
4. Lower resource use on end-user computers.
5. More reliable installation and deployment of an anti-virus solution.
6. Better cross-platform support, including Windows, Macintosh, Linux, and emerging threats in mobile devices.

All of the products evaluated were highly rated for detecting viruses but the committee determined that Sophos performed better defensively than McAfee in regards to the viruses the committee had collected for testing. The committee also determined that Sophos' enterprise management console was simpler, cleaner, and will integrate better with the existing Auburn network, including Active Directory. Sophos also offered more AV product coverage for virtually every O/S present on the AU network.

Because this change will impact the entire University community, the Committee feels it is important we move forward with the purchase and begin implementation as soon as possible. Doing so will allow plenty of time for migration and debugging before the June 8th McAfee expiration date. The committee feels that a purchase decision before December 19, 2008 will allow adequate time for campus-wide implementation of the new product.

If requested, we will answer any questions or concerns from the IT Directors or distributed management teams. Sophos has also offered to come to AU and have a face to face if needed.

Anti-Virus Evaluation Committee