ANTIVIRUS EVALUATION GUIDE

VIPRE® AntivirusBusiness

Make the Right Choice the First Time

As an IT administrator supporting the needs of faculty, students and staff in higher education, you face a unique set of challenges. You may be managing a network supporting thousands or tens of thousands of users, but unlike your peers in the private sector, your diverse user base creates a set of security challenges like no other.

Add to that decreasing budgets, limited staff, geographically dispersed worksites, lack of site-by-site management, time constraints, board of trustees scrutiny, growing dependence on e-learning solutions, the introduction of new devices like iPads and tablet PCs to the classroom and mounting privacy concerns. All of this underscores the critical importance of selecting an antivirus that keeps your network free of malware.

The key to choosing the antivirus solution that's right for your academic institution is implementing an easy-to-deploy and easy-to-replicate testing curriculum that enables you to most accurately assess each solution's capabilities.

The VIPRE Antivirus team at ThreatTrack Security has developed this **Antivirus Evaluation Guide** to help you do just that – and we've made it as simple as 1, 2, 3:

1. Set up a machine to install the management console software to evaluate the installation and configuration process. Refer to your installation documents to ensure that the product is correctly installed and configured.

2. Pick a sample of the different types of machines that you manage (e.g., Windows 7 workstations, Windows XP workstations, servers, laptops). After setting up the management console, deploy agents/clients to these machines for a fair test of how the software will behave on your etwork.

3. Once you install the agents/clients on your test machines, you are ready to start comparing antivirus solutions.

VIPRE® AntivirusBusiness™

Consider all Users

Choosing the best antivirus engine for your specific environment can be a challenging task. Selecting the wrong solution and having to replace it is time-consuming, incredibly costly and a huge hit to an IT admin's professional reputation within an institution.

For a complete and thorough evaluation, we suggest you assess solutions from both the administrator and the end user's point of view. There is nothing more frustrating than choosing a product that is difficult to administer or causes issues with users that generate constant calls to the help desk. A proper evaluation as outlined below will help you avoid these pitfalls.

The Antivirus Evaluation Guide includes:

Administrator Usability Criteria compiled from antivirus user specifications and other common security industry requirements you should evaluate. Feel free to add specific criteria that are important to you or to address known issues within your network. The critical component of the Administrator Usability Criteria is to always ensure that you test each solution in the same manner, so you can rely on your findings when it comes time to select a new antivirus and subsequently, to make your recommendations and budget requests.

End User Usability Scenarios will help you assess how your users will experience each antivirus solution. It's important to consider each solution's performance and impact on as many system configurations and user settings as possible. This way you'll know exactly how faculty, students and staff will be impacted by antivirus agents deployed on the machines they use every day.

Administrator Usability Criteria

The Administrator Usability Criteria component of the evaluation is broken down by Installation, Configuration, Deployment and Management tool requirements. Add additional criteria that are important to you, as well as additional columns for each product you evaluate. Provide a value of 1-10 for each criteria. Remember to apply the same standard across all the products you evaluate.

Administrator Usability Criteria

	Product 1	Product 2
Installation		
Ease of installation		
Clear documentation and guidance		
Vendor support provided during evaluation		
Additional criteria		
Configuration		
Pre-configured policy and group templates (servers, workstations, traveling faculty, etc.)		
Flexible policy and group configurations (departments and user types)		
Management rights settings for sites and policies		
Agent updates, even when devices are off-network (laptops)		
Per-policy allowance to scan files on demand		
Control of agent visibility on endpoints (hide tray icon, hide in Add/Remove programs)		
Per-policy exclusions (always allow) for folders, files and programs		
Firewall templates to assign to policies		
Endpoint email client protection		
Flexible update configurations		
Additional criteria		
Deployment		
Grouping of machines (AD groups, IP ranges, machine names)		
Built-in uninstaller to remove existing agents		
Time required to deploy, ease of deployment		
Size of updates downloaded after first full update		
Additional criteria		
Management tools		
Management console ease of use		
Intuitive dashboard for at-a-glance status assessment (agents not calling in, recently cleaned machines, quarantined files, etc.)		
Customizable executive and technical reports		
Additional criteria		

End User Usability Scenarios

The End User Usability Scenarios test three common indicators that affect user productivity: PC performance, System resources and Spyware detection. These scenarios will help you determine how faculty, students and staff will be impacted by antivirus agents deployed on the machines they use every day.

PC performance

1. With your current antivirus installed, shut down the PC. Start the PC and time how long it takes for the PC to be usable (e.g., the Start Menu is visible). Run the same test on the same type of machine with each product. Which product was the fastest?
2. With your current antivirus installed, reboot the computer to clear out any cache. Once the machine is done booting, launch Internet Explorer and time how long it takes. Run the same test on the same type of machine with each product. Which product was the fastest?
3. With your current antivirus installed, create a folder of documents. Then, compress that folder and time how long the compression takes. Decompress the file to a different location and time that. Run the same test on the same type of machine with each product. Which product was the fastest?
4. Take the uncompressed folder of documents from Test 3, and scan that folder with each product. Which product was the fastest?

PC performance	Product 1	Product 2
1. Time to boot up machine to usable state		
2. Time to open Internet Explorer		
3. Time to compress/decompress a set of files		
4. Time to scan a set of files on demand		
5. Additional criteria		

System resources

1. Run a deep/full system scan on the same type of machine with each product. After you start the scan, wait 2-5 minutes (this allows the scanners to settle into their tasks). Then, bring up Task Manager to measure CPU and memory used on the scanning process. Which product had the lowest resource usage?
2. Perform the same check with the system idle (no scan running). Which product had the lowest CPU and memory utilization?
3. Run each Agent software for a week and see how many users call the help desk and for what reason. Which product had the fewest calls to the help desk?

System resources	Product 1	Product 2
1. Amount of CPU/RAM usage during scans		
2. Amount of CPU/RAM usage during idle		
3. Number of calls to help desk		
4. Additional criteria		

Spyware detection

Spycar* is a suite of tests designed to mimic spyware behavior, but in a benign form. These tests help to evaluate how well an antivirus product defends against spyware threats.

To run a Spycar test with your current antivirus, you first need to download TowTruck (a Spycar tool). This tool will analyze the test results and clean up all Spycar alterations after the test is performed. After downloading TowTruck, choose a Spycar test to attempt to execute with your current antivirus product.

TowTruck will provide you with one of the following test results:

1. **Spycar change allowed** – Sorry, but your anti-spyware tool did not block this test. You are **NOT** protected against this kind of behavior.
2. **Spycar change blocked** – Your antivirus tool blocked this test. That is a good thing!
3. **Spycar test not performed** – Either you did not run this element of Spycar, or your antivirus tool blocked it so thoroughly that Spycar cannot even determine that it was run. The former just means you need to do the test. The latter is a good thing!

Repeat the same test on the same type of machine with each product. Which product blocked the most spyware?

Spyware detection	Product 1	Product 2
Spycar change allowed		
Spycar change blocked		
Spycar test not performed		
Additional criteria		

*The information contained in this document regarding Spycar is taken from the Spycar website listed above. Intelguardians and ThreatTrack Security cannot be held responsible if these files and/or your anti-spyware tool in combination with these files cause any damage to your computer. You download and run these files at your own risk. Download and run these files only if you are sufficiently knowledgeable in the usage of your anti-spyware tool and operating system. Intelguardians cannot and will not provide any help to remove these files or the changes they cause from your computer. Please contact the manufacturer of your anti-spyware tool to seek such help.

Antivirus evaluation results

Now that you have a quantitative assessment of all your antivirus options, it's time to compile the results. By knowing which antivirus meets the unique requirements of your education IT environment, you'll be much more confident recommending the solution you feel is best for your organization. Use the chart below to review and compare each product's performance across all the criteria for which you tested.

	Product 1	Product 2
Admin usability installation		
Admin usability configuration		
Admin usability deployment		
Admin usability management		
End user experience performance		
End user experience resources		
End user experience detections		

Selecting the right antivirus solution is critical for any academic institution. Taking the time to carefully evaluate all your options will ensure you make the right choice the first time.

For more information, visit www.ThreatTrackSecurity.com/VIPRE

VIPRE® AntivirusBusiness™